(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 11 2005 001 666 T5** 2007.05.03

(12) **Veröffentlichung**

der internationalen Anmeldung mit der
(87) Veröffentlichungs-Nr.: **WO 2006/019614**
in deutscher Übersetzung (Art. III § 8 Abs. 2 IntPatÜG)
(21) Deutsches Aktenzeichen: **11 2005 001 666.8**
(86) PCT-Aktenzeichen: **PCT/US2005/024253**
(86) PCT-Anmeldetag: **08.07.2005**
(87) PCT-Veröffentlichungstag: **23.02.2006**
(43) Veröffentlichungstag der PCT Anmeldung
in deutscher Übersetzung: **03.05.2007**

(51) Int Cl.[8]: ***H04L 9/08*** (2006.01)
H04L 9/32 (2006.01)

(30) Unionspriorität:
10/892,280 **14.07.2004** **US**

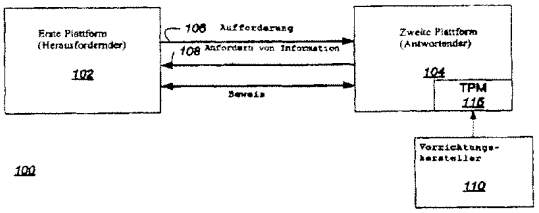
(74) Vertreter:
BOEHMERT & BOEHMERT, 28209 Bremen

(71) Anmelder:
Intel Corp., Santa Clara, Calif., US

(72) Erfinder:
Sutton, James, Portland, Oreg., US; Hall, Clifford, Orangevale, Calif., US; Brickell, Ernie, Portland, Oreg., US; Grawrock, David, Aloha, Oreg., US

(54) Bezeichnung: **Verfahren zum Bereitstellen von privaten Direktbeweis-Schlüsseln in signierten Gruppen für Vorrichtungen mit Hilfe einer Verteilungs-CD**

(57) Hauptanspruch: Verfahren, umfassend:
Erzeugen einer verschlüsselten Datenstruktur, die mit einer Vorrichtung assoziiert ist, wobei die verschlüsselte Datenstruktur einen privaten Schlüssel und ein privates Schlüssel-Digest umfaßt;
Erzeugen eines Identifikators, der auf einem pseudo-zufällig erzeugten Wert beruht, für die verschlüsselte Datenstruktur;
Speichern des Identifikators und der verschlüsselten Datenstruktur in einem signierten Gruppenverzeichnis auf einem entfernbaren Speichermedium; und
Speichern des pseudo-zufälligen Wertes und einer Gruppenzahl, die dem signierten Gruppenverzeichnis entspricht, in einem nichtflüchtigen Speicher innerhalb der Vorrichtung.



Beschreibung

ALLGEMEINER STAND DER TECHNIK

1. GEBIET

[0001] Die vorliegende Erfindung betrifft im allgemeinen die Computersicherheit und genauer das sichere Verteilen kryptographischer Schlüssel an Vorrichtungen in Verarbeitungssystemen.

2. BESCHREIBUNG

[0002] Einige Verarbeitungssystemarchitekturen, welche Inhaltsschutz- und/oder Computersicherheitsmerkmale unterstützen, erfordern, daß speziell geschützte oder „vertrauenswürdige". Softwaremodule eine authentisierte verschlüsselte Kommunikationssitzung mit spezifisch geschützten oder "vertrauenswürdigen" Hardwarevorrichtungen in dem Verarbeitungssystem (wie zum Beispiel Grafiksteuerkarten) erzeugen können. Ein üblicherweise angewendetes Verfahren sowohl zum Identifizieren der Vorrichtung als auch zum gleichzeitigen Erstellen der verschlüsselten Kommunikationssitzung ist die Benutzung eines einseitig authentisierten Diffie-Helman (DH)-Schlüsselaustauschprozesses. In diesem Prozeß wird der Vorrichtung ein einmaliges öffentliches/privates Schlüsselpaar mit Rivest-Shamir-Adelman (RSA)-Algorithmus oder ein einmaliges Schlüsselpaar mit elliptischer Kurvenkryptographie (ECC) zugewiesen. Da dieser Authentifizierungsprozeß jedoch RSA- oder ECC-Schlüssel benutzt, hat die Vorrichtung eine einmalige und beweisbare Identität, was Datenschutzprobleme verursachen kann. Im schlimmsten Fall können diese Probleme zu einem Mangel an Unterstützung seitens der Hersteller von Originalteilen (OEMs) zum Herstellen vertrauenswürdiger Vorrichtungen führen, welche diese Art Sicherheit bereitstellen.

KURZBESCHREIBUNG DER ZEICHNUNGEN

[0003] Die Merkmale und Vorteile der vorliegenden Erfindung werden aus der folgenden ausführlichen Beschreibung der vorliegenden Erfindung offensichtlich. Es zeigen:

[0004] Fig. 1 ein System, das durch eine Plattform gekennzeichnet ist, die mit einem vertrauenswürdigen Plattformmodul (TPM) versehen ist, das gemäß einer Ausführungsform der Erfindung arbeitet;

[0005] Fig. 2 eine erste Ausführungsform der Plattform, die das TPM aus Fig. 1 aufweist;

[0006] Fig. 3 eine zweite Ausführungsform der Plattform, die das TPM aus Fig. 1 aufweist;

[0007] Fig. 4 ein Ausführungsbeispiel eines Computersystems, das mit dem TPM aus Fig. 2 ausgeführt ist;

[0008] Fig. 5 ein Diagramm eines Systems zum Verteilen von Direktbeweis-Schlüsseln in signierten Gruppen gemäß einer Ausführungsform der vorliegenden Erfindung;

[0009] Fig. 6 ein Flußdiagramm, das Schritte eines Verfahrens zum Verteilen von Direktbeweis-Schlüsseln in signierten Gruppen gemäß einer Ausführungsform der vorliegenden Erfindung darstellt;

[0010] Fig. 7 und Fig. 8 Flußdiagramme, die eine Herstellungsaufbauverarbeitung der Vorrichtung gemäß einer Ausführungsform der vorliegenden Erfindung darstellen;

[0011] Fig. 9 ein Flußdiagramm, das eine Herstellungsproduktionsverarbeitung der Vorrichtung gemäß einer Ausführungsform der vorliegenden Erfindung darstellt;

[0012] Fig. 10 und Fig. 11 Flußdiagramme einer Aufbauverarbeitung eines Client-Computersystems gemäß einer Ausführungsform der vorliegenden Erfindung; und

[0013] Fig. 12 ein Flußdiagramm der Verarbeitung eines Client-Computersystems gemäß einer Ausführungsform der vorliegenden Erfindung.

AUSFÜHRLICHE BESCHREIBUNG

[0014] Die Verwendung des auf Direktbeweis beruhenden Diffie-Helman-Schlüsselaustauschprotokolls, damit sich geschützte/vertrauenswürdige Vorrichtungen selbst authentisieren und eine verschlüsselte Kommunikationssitzung mit vertrauenswürdigen Softwaremodulen erstellen können, vermeidet die Erzeugung von einmaliger Identitätsinformation in dem Verarbeitungssystem und vermeidet dadurch Datenschutzprobleme. Jedoch erfordert die direkte Einbettung eines privaten Direktbeweis-Schlüssels in eine Vorrichtung auf einem Herstellungsband mehr geschützten nichtflüchtigen Speicher auf der Vorrichtung als andere Ansätze, was zu erhöhten Vorrichtungskosten führt. Eine Ausführungsform der vorliegenden Erfindung ist ein Verfahren, das ermöglicht, daß private Direktbeweis-Schlüssel (die zum Beispiel zum Signieren benutzt werden) in signierten Gruppen in sicherer Weise auf einem Verteilungs-Kompaktplatten-Nurlesespeicher (CD-ROM oder CD) geliefert und nachfolgend in der Vorrichtung von der Vorrichtung selbst installiert werden. In einer Ausführungsform kann die Reduzierung des Vorrichtungsspeichers, der zur Unterstützung dieser Fähigkeit erforderlich ist, von etwa 300 bis 700 Bytes bis zu etwa 20 bis 25 Bytes betragen. Diese Reduzierung der Menge des nichtflüchtigen Speichers, die zur Umset-

zung des auf Direktbeweis beruhenden Diffie-Helman-Schlüsselaustauschs für Vorrichtungen erforderlich ist, kann zu einer breiteren Anwendung dieser Technik führen.

[0015] Bezugnahmen in der Beschreibung auf "eine Ausführungsform" der vorliegenden Erfindung bedeuten, daß ein bestimmtes Merkmal, eine bestimmte Struktur oder Eigenschaft, die in Verbindung mit der Ausführungsform beschrieben wird, in mindestens einer Ausführungsform der vorliegenden Erfindung enthalten ist. Folglich bezieht sich das Vorkommen des Ausdrucks "in einer Ausführungsform" an verschiedenen Stellen in der Beschreibung nicht unbedingt auf die gleiche Ausführungsform.

[0016] In der folgenden Beschreibung wird eine bestimmte Terminologie benutzt, um bestimmte Merkmale einer oder mehrerer Ausführungsformen der Erfindung zu beschreiben. Zum Beispiel wird "Plattform" als jede beliebige Art von Kommunikationsvorrichtung definiert, die zum Senden und Empfangen von Information geeignet ist. Beispiele verschiedener Plattformen schließen ein, sind jedoch nicht beschränkt oder eingeschränkt auf Computersysteme, persönliche digitale Assistenten, Mobiltelefone, Set-Top-Boxes, Faxgeräte, Drucker, Modems, Router oder dergleichen. Eine "Kommunikationsverbindung" wird allgemein als ein oder mehrere Information tragende Medien definiert, die an eine Plattform angepaßt sind. Beispiele verschiedener Arten von Kommunikationsverbindungen schließen ein, sind jedoch nicht beschränkt oder eingeschränkt auf einen elektrischen Draht oder elektrische Drähte, optische Faser(n), Kabel, Busablaufverfolgung(en) oder drahtlose Signalisierungstechnologie.

[0017] Ein "Herausfordernder" (Challenger) bezieht sich auf jede beliebige Entität (zum Beispiel Person, Plattform, System, Software und/oder Vorrichtung), die eine Verifizierung der Authentizität oder Berechtigung einer anderen Entität anfordert. Im Normalfall wird dies vor dem Offenbaren oder Bereitstellen der angeforderten Information ausgeführt. Ein "Antwortender" (Responder) bezieht sich auf jede beliebige Entität, die aufgefordert worden ist, einen Beweis ihrer Berechtigung, Gültigkeit und/oder Identität bereitzustellen. Der Ausdruck „Vorrichtungshersteller", der mit "bescheinigender Hersteller" austauschbar benutzt werden kann, bezieht sich auf jede beliebige Entität, die eine Plattform oder Vorrichtung herstellt oder konfiguriert.

[0018] Wie hier verwendet, bedeutet einem Herausfordernden "beweisen" oder einen Herausfordernden davon "überzeugen", daß ein Antwortsender eine gewisse kryptographische Information (zum Beispiel digitale Signatur, ein Geheimnis wie einen Schlüssel usw.) besitzt oder kennt, daß basierend auf der dem Herausfordernden offenbarten Information und Nachweis eine hohe Wahrscheinlichkeit besteht, daß der Antwortende kryptographische Information hat. Dies einem Herausfordernden zu beweisen, ohne dem Herausfordernden die kryptographische Information zu „enthüllen" oder zu "offenbaren", bedeutet, daß es für den Herausfordernden basierend auf der dem Herausfordernden offenbarten Information rechnerisch undurchführbar wäre, die kryptographische Information zu bestimmen.

[0019] Solche Beweise werden nachstehend als Direktbeweise bezeichnet. Der Ausdruck "Direktbeweis" bezieht sich auf Nullkenntnisbeweise, wobei diese Beweisarten auf dem Fachgebiet allgemein bekannt sind. Insbesondere ist ein spezifisches Direktbeweis-Protokoll wie hier verwendet Gegenstand der ebenfalls abhängigen Patentanmeldung mit Anmeldenummer 10/306,336, die am 27.11.2002 mit der Bezeichnung „System and Method for Establishing Trust Without Revealing Identity" eingereicht und an den Inhaber der vorliegenden Anmeldung übertragen wurde. Ein Direktbeweis definiert ein Protokoll, in dem ein Aussteller eine Familie vieler Mitglieder definiert, die gemeinsame Eigenschaften teilen, die von dem Aussteller definiert werden. Der Aussteller erzeugt ein Familienpaar eines öffentlichen und privaten Schlüssels (Fpub und Fpri), das für die gesamte Familie steht. Mit Hilfe des Fpri kann der Aussteller auch einen einmaligen privaten Direktbeweis-Signierschlüssel (DPpri) für jedes einzelne Mitglied in der Familie erzeugen. Jede Nachricht, die von einem einzelnen DPpri signiert wird, kann mit Hilfe des öffentlichen Familienschlüssels Fpub verifiziert werden. Jedoch identifiziert solch eine Verifikation nur, daß der Signierer ein Mitglied der Familie ist; es wird keine eindeutig identifizierende Information über das einzelne Mitglied dargelegt. In einer Ausführungsform kann der Aussteller ein Vorrichtungshersteller oder Vertreter sein. Das heißt, der Aussteller kann eine Entität mit der Fähigkeit zum Definieren von Vorrichtungsfamilien basierend auf den gemeinsamen Eigenschaften, zum Erzeugen des öffentlichen/privaten Familienschlüsselpaars und zum Erzeugen und Einführen privater DP-Schlüssel in die Vorrichtungen sein. Der Aussteller kann auch Zertifikate für den öffentlichen Familienschlüssel erzeugen, welche die Quelle des Schlüssels und die Eigenschaften der Vorrichtungsfamilie identifizieren.

[0020] Mit Bezug auf **Fig. 1** ist eine Ausführungsform eines Systems, das durch eine Plattform gekennzeichnet ist, die mit einer vertrauenswürdigen Hardwarevorrichtung (als "vertrauenswürdiges Plattformmodul" oder "TPM" bezeichnet) ausgeführt ist, die gemäß einer Ausführungsform der Erfindung arbeitet, dargestellt. Eine erste Plattform **102** (Herausfordernder) sendet eine Aufforderung **106**, daß eine zweite Plattform **104** (Antwortender) Information über sich selbst bereitstellt. In Antwort auf die Aufforderung **106** stellt die zweite Plattform **104** die angefor-

derte Information **108** bereit.

[0021] Außerdem muß die erste Plattform **102** für eine erhöhte Sicherheit möglicherweise verifizieren, daß die angeforderte Information **108** von einer Vorrichtung kommt, die entweder von einem ausgewählten Vorrichtungshersteller oder einer ausgewählten Gruppe von Vorrichtungsherstellern (nachstehend als "Vorrichtungshersteller **110**" bezeichnet) kommt. Zum Beispiel fordert die erste Plattform **102** in einer Ausführungsform der Erfindung die zweite Plattform **104** heraus, zu zeigen, daß sie kryptographische Information (zum Beispiel eine Signatur) hat, die von dem(den) Vorrichtungshersteller(n) **110** erzeugt ist. Die Herausforderung kann entweder in einer Aufforderung **106** (wie dargestellt) enthalten sein oder in eine getrennte Übertragung sein. Die zweite Plattform **104** antwortet auf die Herausforderung durch Bereitstellen von Information in Form einer Antwort, um die erste Plattform **102** zu überzeugen, daß die zweite Plattform **104** kryptographische Information hat, die von dem(den) Vorrichtungshersteller(n) **110** erzeugt ist, ohne die kryptographische Information zu enthüllen. Die Antwort kann entweder Teil der angeforderten Information **108** (wie dargestellt) oder eine getrennte Übertragung sein.

[0022] In einer Ausführungsform der Erfindung umfaßt die zweite Plattform **104** ein vertrauenswürdiges Platform-Modul (TPM) **115**. Das TPM **115** ist eine kryptographische Vorrichtung, die von dem(den) Vorrichtungshersteller(n) **110** hergestellt wird. In einer Ausführungsform der Erfindung umfaßt das TPM **115** einen Prozessor mit einer kleinen Menge von Speicher auf einem Chip, der innerhalb eines Gehäuses eingekapselt ist. Das TPM **115** ist konfiguriert, um der ersten Plattform **102** Information bereitzustellen, die sie dazu befähigen würde, zu bestimmen, daß eine Antwort von einem gültigen TPM gesendet wird. Die benutzte Information ist Inhalt, der es nicht wahrscheinlich macht, daß die Identität des TPM oder der zweiten Plattform bestimmt werden kann.

[0023] Fig. 2 stellt eine erste Ausführungsform der zweiten Plattform **104** mit dem TPM **115** dar. Für diese Ausführungsform der Erfindung umfaßt die zweite Plattform **104** einen Prozessor **202**, der mit dem TPM **115** verbunden ist. Im allgemeinen ist der Prozessor **202** eine Vorrichtung, die Information verarbeitet. Zum Beispiel kann der Prozessor **202** in einer Ausführungsform der Erfindung als ein Mikroprozessor, digitaler Signalprozessor, eine Mikrosteuerung oder sogar Zustandsmaschine ausgeführt sein. Als Alternative kann der Prozessor **202** in einer anderen Ausführungsform der Erfindung als eine programmierbare oder hartcodierte Logik, wie feldprogrammierbare Gate-Arrays (FPGAs); eine Transistor-Transistor-Logik (TTL) oder sogar eine anwendungsspezifische integrierte Schaltung (ASIC) ausgeführt sein.

[0024] Hierin umfaßt die zweite Plattform **104** ferner eine Speichereinheit **206**, um die Speicherung kryptographischer Information wie eines oder mehrere der Folgenden zu ermöglichen: Schlüssel, Hash-Werte (Streuwerte), Signaturen, Zertifikate usw. Ein Hash-Wert von „X" kann als "HASH(X)" dargestellt werden. Es wird berücksichtigt, daß solche Information in dem internen Speicher **220** des TPMs **115** anstatt der Speichereinheit **206** gespeichert werden kann, wie in Fig. 3 dargestellt. Die kryptographische Information kann verschlüsselt werden, besonders wenn sie außerhalb des TPMs **115** gespeichert wird.

[0025] Fig. 4 stellt eine Ausführungsform einer Plattform dar, die ein Computersystem **300** aufweist, das mit dem TPM **115** aus Fig. 2 implementiert ist. Das Computersystem **300** umfaßt einen Bus **302** und einen Prozessor **310**, der mit dem Bus **302** verbunden ist. Das Computersystem **300** umfaßt ferner eine Hauptspeichereinheit **304** und eine statische Speichereinheit **306**.

[0026] Hierin ist die Hauptspeichereinheit **304** ein flüchtiger Halbleiterspeicher zum Speichern von Information und Befehlen, die von dem Prozessor **310** ausgeführt werden. Der Hauptspeicher **304** kann auch zum Speichern temporärer Variablen oder anderer Zwischeninformation während der Ausführung von Befehlen durch den Prozessor **310** sein. Die statische Speichereinheit **306** ist ein nichtflüchtiger Halbleiterspeicher zum Speichern von Information und Befehlen von dauerhafterer Natur für den Prozessor **310**. Beispiele eines statischen Speichers **306** schließen ein, sind jedoch nicht beschränkt oder eingeschränkt auf Nurlesespeicher (ROM). Sowohl die Hauptspeichereinheit **304** als auch die statische Speichereinheit **306** sind mit dem Bus **302** verbunden.

[0027] In einer Ausführungsform der Erfindung umfaßt ein Computersystem **300** ferner eine Datenspeichervorrichtung **308**, wie eine Magnetplatte oder optische Platte, und ihr entsprechendes Laufwerk kann auch mit dem Computersystem **300** zum Speichern von Information und Befehlen verbunden sein.

[0028] Das Computersystem **300** kann auch über den Bus **302** mit der Grafiksteuervorrichtung **314** verbunden sein, die eine Anzeige (nicht dargestellt) wie eine Kathodenstrahlröhre (CRT), Flüssigkristallanzeige (LCD) oder jeden beliebigen Flachbildschirm zum Anzeigen von Information für einen Endbenutzer steuert. In einer Ausführungsform kann gewünscht werden, daß die Grafiksteuerung oder eine andere periphere Vorrichtung eine authentisierte verschlüsselte Kommunikationssitzung mit einem Softwaremodul erstellt, das von dem Prozessor ausgeführt wird.

[0029] In der Regel kann eine alphanumerische Ein-

gabevorrichtung **316** (zum Beispiel eine Tastatur, Kleintastatur usw.) mit dem Bus **302** verbunden sein, um dem Prozessor **310** Information und/oder Befehlsauswahlen mitzuteilen. Eine andere Art Benutzereingabevorrichtung ist die Kursorsteuereinheit **318**, wie z.B. eine Maus, eine Steuerkugel, Berührungsfeld, Eingabestift oder Kursorrichtungstasten, um dem Prozessor **310** Richtungsinformation und Befehlsauswahlen mitzuteilen und die Kursorbewegung auf der Anzeige **314** zu steuern.

[0030] Eine Kommunikationsschnittstelleneinheit **320** ist auch mit dem Bus **302** verbunden. Beispiele einer Schnittstelleneinheit **320** sind ein Modem, eine Netzwerkschnittstellenkarte oder andere gut bekannte Schnittstellen, die zum Verbinden mit einer Kommunikationsverbindung benutzt werden, die Teil eines lokalen Netzes oder Fernnetzes sind. Auf diese Weise kann das Computersystem **300** mit einer Anzahl von Kunden und/oder Servern über eine herkömmliche Netzwerkinfrastruktur wie zum Beispiel das Intranet eines Unternehmens und/oder das Internet verbunden werden.

[0031] Es versteht sich, daß für bestimmte Ausführungen ein Computersystem wünschenswert sein kann, das weniger oder mehr Ausstattung aufweist als das beschriebene. Folglich variiert die Konfiguration des Computersystems **300** von Ausführung zu Ausführung abhängig von zahlreichen Faktoren, wie Preiseinschränkungen, Leistungsanforderungen, technologische Verbesserungen und/oder anderen Umständen.

[0032] In mindestens einer Ausführungsform kann das Computersystem **300** die Verwendung speziell geschützter „vertrauenswürdiger" Softwaremodule (zum Beispiel manipulationssichere Software oder Systeme mit der Fähigkeit zum Ausführen geschützter Programme) unterstützen, die in dem Hauptspeicher **304** und/oder Massenspeichervorrichtung **308** gespeichert sind und von dem Prozessor **310** ausgeführt werden, um spezifische Aktivitäten sogar bei Vorhandensein einer anderen feindlichen Software in dem System auszuführen. Einige dieser vertrauenswürdigen Softwaremodule erfordern einen gleichermaßen „vertrauenswürdigen" geschützten Zugang nicht nur zu anderen Plattformen, sondern auch zu einer oder mehreren Vorrichtungen innerhalb der gleichen Plattform, wie zum Beispiel der Grafiksteuerung **314**. Im allgemeinen erfordert solch ein Zugang, daß das vertrauenswürdige Softwaremodul die Fähigkeiten und/oder spezifische Identität der Vorrichtung identifizieren und dann eine verschlüsselte Sitzung mit der Vorrichtung einrichten kann, um den Austausch von Daten zu ermöglichen, die von einer anderen Software in dem System nicht ausspioniert oder verfälscht werden können.

[0033] Ein Verfahren des Standes der Technik sowohl zum Identifizieren der Vorrichtung als auch zum gleichzeitigen Erstellen der verschlüsselten Sitzung ist die Benutzung eines einseitig authentisierten Diffie-Helman (DH) -Schlüsselaustauschprozesses. In diesem Prozeß wird der Vorrichtung ein einmaliges öffentliches/privates RSA- oder ECC-Schlüsselpaar zugewiesen. Die Vorrichtung enthält den privaten Schlüssel und schützt ihn, während der öffentliche Schlüssel zusammen mit Authentifizierungszertifikaten an das Softwaremodul freigegeben werden kann. Während des DH-Schlüsselaustauschprozesses signiert die Vorrichtung eine Nachricht mittels ihres privaten Schlüssels, den das Softwaremodul mit Hilfe des entsprechenden öffentlichen Schlüssels verifizieren kann. Dies ermöglicht, daß das Softwaremodul authentisieren kann, daß die Nachricht tatsächlich aus der fraglichen Vorrichtung gekommen ist.

[0034] Da dieser Authentifizierungsprozeß jedoch RSA- oder ECC-Schlüssel benutzt, hat die Vorrichtung eine einmalige und nachweisbare Identität. Jedes beliebige Softwaremodul, das die Vorrichtung dazu bringen kann, um eine Nachricht mit ihrem privaten Schlüssel zu signieren, kann beweisen, daß diese spezifische einmalige Vorrichtung in dem Computersystem vorhanden ist. Da Vorrichtungen selten zwischen Verarbeitungssystemen wandern, stellt dies auch eine beweisbare eindeutige Computersystemidentität dar. Darüber hinaus repräsentiert der öffentliche Schlüssel der Vorrichtung selbst einen konstanten eindeutigen Wert; quasi einen permanenten "Cookie". In manchen Fällen können diese Eigenschaften als ein bedeutendes Datenschutzproblem verstanden werden.

[0035] Ein alternativer Ansatz ist in der ebenfalls abhängigen Patentanmeldung mit Anmeldenummer 10/???, ??? beschrieben, die am ?.?. 2004 mit der Bezeichnung "An Apparatus and Method for Establishing an Authenticated Encrypted Session with a Device Without Exposing Privacy-Sensitive Information" eingereicht und auf den Inhaber der vorliegenden Anmeldung übertragen wurde. In diesem Ansatz wird die Verwendung von RSA- oder ECC-Schlüsseln in dem einseitig authentisierten Diffie-Helman-Prozeß durch Direktbeweis-Schlüssel ersetzt. Eine Vorrichtung, welche diesen Ansatz anwendet, kann als zu einer spezifischen Familie von Vorrichtungen zugehörig authentisiert werden, was Zusicherungen über das Verhalten oder die Vertrauenswürdigkeit der Vorrichtung umfassen kann. Der Ansatz legt keinerlei eindeutig identifizierende Information offen, die benutzt werden könnte, um eine eindeutige Identität zu erstellen, die das Verarbeitungssystem repräsentiert.

[0036] Obwohl dieser Ansatz gut funktioniert, erfordert er zusätzlichen Speicher in der Vorrichtung, um den privaten Direktbeweis-Schlüssel zu halten, der größer als ein RSA- oder ECC-Schlüssel sein kann. Um die Probleme dieses zusätzlichen Speichererfor-

dernisses abzuschwächen, definieren Ausführungsformen der vorliegenden Erfindung ein System und Verfahren zur Gewährleistung, daß die Vorrichtung den privaten Direktbeweis-Schlüssel aufweist, sie den Schlüssel benötigt, ohne im wesentlichen zusätzlichen Speicher in der Vorrichtung zu benötigen. In einer Ausführungsform werden die DP-Schlüssel dem Client-Computersystem in signierten Gruppen geliefert.

[0037] In mindestens einer Ausführungsform der vorliegenden Erfindung speichert ein Vorrichtungshersteller nur eine pseudo-zufällige 128-Bit-Zahl in einer Vorrichtung, während die Vorrichtung auf dem Herstellungsband hergestellt wird, während ein viel größerer privater Direktbeweis-Schlüssel (DPpri) verschlüsselt und mit Hilfe einer Verteilungs-CD bereitgestellt werden kann. Andere Ausführungsformen können eine Zahl in der Vorrichtung speichern, die länger oder kürzer als 128 Bit ist. Dieser Prozeß gewährleistet, daß nur eine bestimmte Vorrichtung ihren zugewiesenen DPpri-Schlüssel entschlüsseln und benutzen kann.

[0038] In mindestens einer Ausführungsform der vorliegenden Erfindung können verschlüsselte DPpri-Datenstrukturen, die "Schlüssel-Blobs" genannt werden, in Gruppenverzeichnissen geliefert werden, die von einem Vorrichtungshersteller signiert werden. Das gesamte Gruppenverzeichnis muß zur Vorrichtung geliefert werden, die nur ihren eigenen verschlüsselten Schlüssel-Blob extrahiert. Ein Angreifer kann basierend auf der zeitlichen Abstimmung von Angriffen nicht folgern, welcher Schlüssel-Blob ausgewählt wurde, da die Vorrichtung das gesamte Verzeichnis syntaktisch analysieren muß und mit der Verarbeitung des extrahierten Schlüssel-Blobs nicht beginnen darf, bis das gesamte Verzeichnis syntaktisch analysiert worden ist. Durch Signieren des Verzeichnisses und Fordern, daß die Vorrichtung die Signatur vor der Verarbeitung ihres Schlüssel-Blobs verifiziert, kann gewährleistet werden, daß ein Angreifer zur Prüfung der Antwort der Vorrichtung keine Mehrfachkopien eines einzigen Schlüssel-Blobs liefern kann. In einer Ausführungsform kann ein Angreifer bestenfalls bestimmen, daß die Vorrichtung ein Mitglied der Gruppe ist. In einer Ausführungsform speichert die Vorrichtung einen pseudozufälligen Wert einer vorbestimmten Größe (zum Beispiel 128 Bit), einen Gruppenidentifikator (zum Beispiel 4 Byte) und einen 20-Byte-Streuwert (Hash) des öffentlichen Gruppenschlüssels des Vorrichtungsherstellers für eine Gesamtanzahl von etwa 40 Datenbytes.

[0039] Fig. 5 ist ein Diagramm eines Systems zum Verteilen von Direktbeweis-Schlüsseln in signierten Gruppen gemäß einer Ausführungsform der vorliegenden Erfindung. Es gibt drei Entitäten in diesem System, ein geschütztes Vorrichtungsherstellungssystem **502**, ein Vorrichtungsherstellungs-Produktionssystem **503** und ein Client-Computersystem **504**. Das geschützte Vorrichtungsherstellungssystem umfaßt ein Verarbeitungssystem, das in dem Aufbauprozeß vor der Herstellung einer Vorrichtung **506** benutzt wird. Das geschützte System **502** kann von einem Vorrichtungshersteller oder einer anderen Entität derart betrieben werden, daß das geschützte System vor Angriffen von Hackern außerhalb des Vorrichtungsherstellungsortes geschützt wird (zum Beispiel ein geschlossenes System ist). Das Herstellungsproduktionssystem **503** kann bei der Herstellung der Vorrichtungen benutzt werden. In einer Ausführungsform können das geschützte System und das Produktionssystem das gleiche System sein. Die Vorrichtung **506** umfaßt jede beliebige Hardwarevorrichtung zur Einbeziehung in das Client-Computersystem (zum Beispiel eine Speichersteuerung, eine periphere Vorrichtung wie eine Grafiksteuerung, eine I/O-Vorrichtung, andere Vorrichtungen usw.). In Ausführungsformen der vorliegenden Erfindung umfaßt die Vorrichtung einen pseudo-zufälligen Wert RAND **508** und eine Gruppenzahl **509**, die in einem nichtflüchtigen Speicher der Vorrichtung gespeichert ist.

[0040] Das geschützte Herstellungssystem weist eine geschützte Datenbank **510** und eine Erzeugungsfunktion **512** auf. Die geschützte Datenbank umfaßt eine Datenstruktur zum Speichern einer Vielzahl pseudo-zufälliger Werte (mindestens einen pro herzustellender Vorrichtung), die durch die Erzeugungsfunktion **512** in einer unten beschriebenen Weise erzeugt werden. Die Erzeugungsfunktion umfaßt eine Logik (entweder in Software oder Hardware umgesetzt), um eine Datenstruktur zu erzeugen, die hierin als ein Schlüssel-Blob **514** bezeichnet wird. Das Schlüssel-Blob **514** umfaßt mindestens drei Datenelemente. Ein einmaliger privater Direktbeweis-Schlüssel (DPpri) umfaßt einen kryptographischen Schlüssel, der von einer Vorrichtung zum Signieren benutzt werden kann. Die private DP-Übersicht **516** (DPpri-Übersicht) umfaßt eine Nachrichtenübersicht von DPpri gemäß jedem beliebigen gut bekannten Verfahren zum Erzeugen einer sicheren Nachrichtenübersicht, wie beispielsweise SHA-1. Einige Ausführungsformen können einen pseudozufälligen Initialisierungsvektor (IV) **518** aufweisen, der zu Kompatibilitätszwecken einen Bitstrom als Teil des Schlüssel-Blobs umfaßt. Wenn eine Stromchiffrierung zur Verschlüsselung benutzt wird, dann wird der IV in einem gut bekannten Verfahren zur Verwendung eines IV in einem Stromchiffrierverfahren benutzt. Wenn eine Blockchiffrierung zur Verschlüsselung benutzt wird, dann wird der IV als Teil der zu verschlüsselnden Nachricht benutzt, wodurch jedes Exemplar der Verschlüsselung anders gemacht wird.

[0041] In Ausführungsformen der vorliegenden Erfindung erzeugt das geschützte Herstellungssystem einen oder mehrere Schlüssel-Blobs (wie nachstehend ausführlich beschrieben) und speichert die

Schlüssel-Blobs in den Gruppenverzeichnissen **515** in einer Schlüssel-Blob-Datenbank **520** auf einer CD **522**. In einer Ausführungsform kann es in jedem Gruppenverzeichnis viele Schlüssel-Blobs und viele Gruppenverzeichnisse auf einer einzigen CD in jeder beliebigen Kombination geben, wobei die einzige Einschränkung die physikalische Speichergrenze der CD ist. Folglich umfaßt jedes Gruppenverzeichnis mehrere Schlüssel-Blobs. Die CD wird dann durch typische physikalische Kanäle an Computersystemhersteller, Computervertreiber, Client-Computersystem-Verbraucher und andere verteilt. Wenngleich eine CD hierin als Speichermedium beschrieben wird, kann jedes beliebige geeignete entfernbare Speichermedium (zum Beispiel eine digitale vielseitige Platte (DVD) oder anderes Medium) benutzt werden.

[0042] Ein Client-Computersystem **504**, das die Verwendung eines Direktbeweis-Protokolls zur Authentifizierung und zum Schlüsselaustausch einer Kommunikationssitzung mit der Vorrichtung **506** wünscht, die innerhalb des Systems **504** enthalten ist, kann ein ausgewähltes Gruppenverzeichnis **515** aus der Schlüssel-Blob-Datenbank **520** auf der CD lesen, sobald die CD in ein CDROM-Laufwerk (nicht dargestellt) des Client-Computersystems eingelegt ist. Die Schlüssel-Blob-Daten können von dem Gruppenverzeichnis erhalten und von der Vorrichtung benutzt werden, um einen lokalisierten Schlüssel-Blob **524** (wie unten beschrieben) zum Gebrauch bei der Implementierung des Direktbeweis-Protokolls zu erzeugen. In Ausführungsformen der vorliegenden Erfindung wird ein gesamtes Gruppenverzeichnis, das mehrere Schlüssel-Blobs umfaßt, von der Vorrichtung auf einmal verarbeitet, wobei ein Angreifer nicht bestimmen kann, welches spezifische Schlüssel-Blob derzeit benutzt wird, um den verschlüsselten lokalisierten Schlüssel-Blob zu erzeugen. Die Vorrichtungstreibersoftware **526** wird von dem Client-Computersystem ausgeführt, um die Vorrichtung **506** zu starten und zu steuern.

[0043] In Ausführungsformen der vorliegenden Erfindung kann es vier unterschiedliche Betriebsstufen geben. Fig. 6 ist ein Flußdiagramm, das die Schritte eines Verfahrens zum Verteilen von Direktbeweis-Schlüsseln gemäß einer Ausführungsform der vorliegenden Erfindung darstellt. Gemäß Ausführungsformen der vorliegenden Erfindung können bei jedem Schritt bestimmte Funktionen ausgeführt werden. An einem Vorrichtungsherstellungsort gibt es mindestens zwei Stufen: die Aufbaustufe **602** und die Herstellungsproduktionsstufe **604**. Die Aufbaustufe wird hierin mit Bezug auf Fig. 7 beschrieben. Die Herstellungsproduktionsstufe wird hierin mit Bezug auf Fig. 8 beschrieben. An einem Verbraucherort, an dem sich das Client-Computersystem befindet, gibt es mindestens zwei Stufen: die Aufbaustufe **606** und die Benutzungsstufe **608**. Die Aufbaustufe des Client-Computersystems wird hierin mit Bezug auf Fig. 9 beschrieben. Die Benutzungsstufe des Client-Computersystems wird hierin mit Bezug auf Fig. 10 beschrieben.

[0044] Fig. 7 und Fig. 8 sind Flußdiagramme **700** und **800**, die eine Herstellungsaufbauverarbeitung der Vorrichtung gemäß einer Ausführungsform der vorliegenden Erfindung darstellen. In einer Ausführungsform kann ein Vorrichtungshersteller diese Handlungen mit Hilfe eines geschützten Herstellungssystems **502** ausführen. Bei Block **701** erzeugt der Vorrichtungshersteller ein Direktbeweis-Familienschlüsselpaar (Fpub und Fpri) für jede Klasse von herzustellenden Vorrichtungen. Jede einmalige Vorrichtung weist einen entsprechenden DPpri-Schlüssel auf, so daß eine Signatur, die mit Hilfe des DPpri erzeugt wird, von dem Fpub verifiziert werden kann. Eine Vorrichtungsklasse kann basierend auf der Versionsnummer oder anderen Eigenschaften der Vorrichtungen jeden beliebigen Satz oder untergeordneten Satz von Vorrichtungen wie eine ausgewählte Produktlinie (das heißt, Vorrichtungsart) oder untergeordnete Sätze einer Produktlinie umfassen. Das Familienschlüsselpaar dient dem Gebrauch der Vorrichtungsklasse, für welche es erzeugt wurde.

[0045] Bei Block **702** erzeugt der Vorrichtungshersteller ein RSA-Schlüsselpaar (Gpri, Gpub), das zum Signieren und Verifizieren des Gruppenverzeichnisses benutzt wird. In anderen Ausführungsformen kann statt RSA jedes beliebige digitale Signatursystem benutzt werden. Dieses Schlüsselpaar ist unabhängig von dem Familienschlüsselpaar, das in Block **701** erzeugt wird, und kann für alle Vorrichtungsgruppierungen benutzt werden, die von dem Vorrichtungshersteller erzeugt werden. Bei Block **703** wählt der Vorrichtungshersteller eine gewünschte Gruppengröße aus. Die Gruppengröße kann die Anzahl von Vorrichtungen in der Familie sein, die gruppiert wird. Die Gruppengröße wird groß genug ausgewählt, so daß sich eine einzelne Vorrichtung innerhalb der Gruppe „verstecken" kann, jedoch nicht so groß, daß während der Schlüssel-Blob-Extraktionsverarbeitung von der Vorrichtung unangemessen viel Zeit verbraucht wird. In einer Ausführungsform kann die Gruppengröße mit 5.000 Vorrichtungen ausgewählt werden. In anderen Ausführungsformen können andere Größen benutzt werden.

[0046] Der Vorrichtungshersteller kann dann die Anzahl von Vorrichtungsschlüsseln erzeugen, die von der Gruppengröße spezifiziert wird. Jeder Gruppe mit einer Anzahl von Vorrichtungen, die von der Gruppengröße spezifiziert wird, kann mit einer Gruppenzahl bezeichnet werden. Für jede Vorrichtung, die für eine gegebene Gruppe herzustellen ist, können die Erzeugungsfunktion **512** oder anderen Module des geschützten Herstellungssystems **502** die Blöcke **704** aus Fig. 7 bis **802** aus Fig. 8 ausführen. Zuerst

erzeugt die Erzeugungsfunktion bei Block **704** einen einmaligen pseudo-zufälligen Wert (RAND) **508**. In einer Ausführungsform beträgt die Länge des RAND 128 Bit. In anderen Ausführungsformen können andere Werte benutzt werden. In einer Ausführungsform können die pseudo-zufälligen Werte für eine Anzahl von Vorrichtungen im Vorfeld erzeugt werden. Bei Block **706** erzeugt die Erzeugungsfunktion mit Hilfe einer Einwegfunktion f, die von der Vorrichtung unterstützt wird, einen symmetrischen Verschlüsselungsschlüssel SKEY aus dem eindeutigen RAND-Wert (SKEY = f(RAND). Die Einwegfunktion kann ein beliebiger bekannter Algorithmus sein, der zu diesem Zweck geeignet ist (zum Beispiel SHA-1, MGF1, Datenverschlüsselungsstandard (DES), Dreifach-DES usw.). Bei Block **708** erzeugt die Erzeugungsfunktion ein Identifikator (ID)-Etikett, das benutzt wird, um das Schlüssel-Blob **515** dieser Vorrichtung auf der Verteilungs-CD zu referenzieren, indem der SKEY benutzt wird, um einen „Nulleintrag" (zum Beispiel eine kleine Anzahl von Nullbytes) (Vorrichtungs-ID = Verschlüsseln von (0..0) mit Hilfe von SKEY zu verschlüsseln. In anderen Ausführungsformen können andere Art und Weisen zum Erzeugen der Vorrichtungs-ID benutzt werden oder andere Werte können von dem SKEY verschlüsselt werden.

[0047] Danach erzeugt die Erzeugungsfunktion in Block **710** den privaten DP-Signierschlüssel, der mit dem öffentlichen Familienschlüssel (Fpub) der Vorrichtung in Beziehung steht. Bei Block **712** hashed die Erzeugungsfunktion DPpri, um ein DPpri-Digest mittels bekannter Verfahren (zum Beispiel mittels SHA-1 oder einem anderen Hash-Algorithmus) zu erzeugen. Bei Block **714** bildet die Erzeugungsfunktion eine Schlüssel-Blob-Datenstruktur für die Vorrichtung. Das Schlüssel-Blob weist mindestens DPpri und den DPpri-Digest auf. In einer Ausführungsform weist das Schlüssel-Blob auch einen zufälligen Initialisierungsvektor (IV) auf, der mehrere pseudo-zufällig erzeugte Bits aufweist. Diese Werte können unter Verwendung von SKEY verschlüsselt werden, um ein verschlüsseltes Schlüssel-Blob **514** zu erzeugen. Bei Block **716** können die in Block **708** erzeugte Vorrichtungs-ID und das in Block **714** erzeugte verschlüsselte Schlüssel-Blob **514** in einem Verzeichnis in der Schlüssel-Blob-Datenbank **520** gespeichert und auf der Verteilungs-CD **522** freigegeben werden. In einer Ausführungsform kann das Verzeichnis in der Schlüssel-Blob-Datenbank mit der Vorrichtungs-ID gekennzeichnet werden.

[0048] Die Verarbeitung geht bei Block **801** in Fig. 8 weiter. In Block **801** können der derzeitige RAND-Wert und die derzeitige Gruppenzahl für die Gruppe, zu der die Vorrichtung gehört, in der geschützten Datenbank **510** gespeichert werden. In Block **802** können der SKEY und DPpri gelöscht werden, da sie von der Vorrichtung in dem Feld erneut erzeugt werden. Die Gruppenzahl kann für jede nachfolgende Gruppe von hergestellten Vorrichtungen erhöht werden. Die Erschaffung des DPpri-Digest und die nachfolgende Verschlüsselung durch den SKEY sind derart gestaltet, daß die Inhalte des DPpri von keiner Entität bestimmt werden können, die nicht im Besitz des SKEY ist, und derart, daß die Inhalte des Schlüssel-Blobs von keiner Entität modifiziert werden können, die nicht im Besitz des SKEY ist, ohne danach von einer Entität erfasst zu werden, die in Besitz des SKEY ist. In anderen Ausführungsformen können andere Verfahren zum Bereitstellen dieses Datenschutzes und Integritätsschutzes angewendet werden. In einigen Ausführungsformen kann der Integritätsschutz nicht erforderlich sein und es könnte ein Verfahren, das nur den Datenschutz bereitstellt, angewendet werden. In diesem Fall wäre der Wert des DPpri-Digest nicht notwendig.

[0049] Wenn der gesamte Datensatz von Schlüssel-Blobs für eine Gruppe von Vorrichtungen erzeugt worden ist, kann zumindest die Schlüssel-Blob-Datenbank **520** dieser Gruppe signiert und auf eine gewöhnliche Verteilungs-CD gebrannt werden, die mit der jeweiligen Vorrichtung vertrieben wird (in einer Ausführungsform kann ein Eintrag der Schlüssel-Blob-Datenbank für jede Vorrichtung benutzt werden, die von dem Vorrichtungs-ID-Feld indexiert wird). Folglich erzeugt der Vorrichtungshersteller bei Block **804** ein Gruppenverzeichnis **515**. Das Gruppenverzeichnis umfaßt die Gruppenzahl, den öffentlichen Gruppenschlüssel Gpub, die Gruppengröße und die Schlüssel-Blob-Verzeichnisse der gesamten Gruppe (<Group Number, Gpub, Group Size, <Device IDI, Encrypted Keyblobl>, <Device ID2, Encrypted Keyblob2>, ...>). Bei Block **806** signiert der Vorrichtungshersteller das Gruppenverzeichnis mit Hilfe des privaten Gruppenschlüssels Gpri und hängt die digitale Signatur an das Gruppenverzeichnis an. In Block **808** kann das signierte Gruppenverzeichnis zu der Schlüssel-Blob-Datenbank auf der Verteilungs-CD hinzugefügt werden. In einer Ausführungsform umfaßt die Verteilungs-CD auch ein Schlüsselabruf-Utility-Softwaremodul zur zukünftigen Verarbeitung auf dem Client-Computersystem, dessen Benutzung nachstehend ausführlicher beschrieben wird.

[0050] Zu jedem beliebigen Zeitpunkt nach Block **802** kann die geschützte Datenbank von RAND- und Gruppenzahl-Wertpaaren sicher auf das Herstellungsproduktionssystem **503** hochgeladen werden, das die RAND- und Gruppenzahl-Werte während des Herstellungsprozesses in den Vorrichtungen speichert. Sobald dieser Upload verifiziert worden ist, können die RAND-Werte aus dem geschützten Herstellungssystem **502** sicher gelöscht werden.

[0051] Fig. 9 ist ein Flußdiagramm **900**, das eine Herstellungsproduktionsverarbeitung der Vorrichtung gemäß einer Ausführungsform der vorliegenden Erfindung darstellt. Während die Vorrichtungen in einer

Produktionslinie hergestellt werden, wählt das Herstellungsproduktionssystem bei Block **902** ein unbenutztes RAND- und Gruppenzahl-Wertepaar aus der geschützten Datenbank aus. Der ausgewählte RAND- und Gruppenzahl-Wert kann dann in dem nichtflüchtigen Speicher in einer Vorrichtung gespeichert werden. In einer Ausführungsform umfaßt der nichtflüchtige Speicher ein TPM. In Block **904** kann ein Streuwert des öffentlichen Gruppenschlüssels Gpub auch in dem nichtflüchtigen Speicher der Vorrichtung gespeichert werden. In Block **906** zerstört das Herstellungsproduktionssystem sämtliche Aufzeichnungen des RAND-Wertes dieser Vorrichtung in der geschützten Datenbank, sobald die Speicherung des RAND-Wertes in der Vorrichtung erfolgreich ist. An diesem Punkt wird die einzige Kopie des RAND-Wertes in der Vorrichtung gespeichert.

[0052] In einer alternativen Ausführungsform kann der RAND-Wert während der Herstellung einer Vorrichtung erzeugt und danach an das geschützte Herstellungssystem für die Berechnung eines Schlüssel-Blobs gesendet werden.

[0053] In einer anderen Vorrichtung kann der RAND-Wert auf der Vorrichtung erzeugt werden und die Vorrichtung und das geschützte Herstellungssystem können in ein Protokoll verknüpft sein, um den DPpri-Schlüssel mit Hilfe eines Verfahrens zu erzeugen, das den DPpri-Schlüssel außerhalb der Vorrichtung nicht enthüllt. Dann kann die Vorrichtung die Vorrichtungs-ID, den SKEY und den Schlüssel-Blob erzeugen. Die Vorrichtung leitet die Vorrichtungs-ID und den Schlüssel-Blob an das Herstellungssystem zur Speicherung in der geschützten Datenbank **510** weiter. In diesem Verfahren weist das Herstellungssystem am Ende die gleiche Information (Vorrichtungs-ID, Schlüssel-Blob) in der geschützten Datenbank auf, kennt jedoch nicht die Werte von RAND oder von DPpri.

[0054] Fig. 10 und Fig. 11 sind Flußdiagramme **1000** und **1100** einer Aufbauverarbeitung eines Client-Computersystems gemäß einer Ausführungsform der vorliegenden Erfindung. Ein Client-Computersystem kann diese Handlungen als Teil des Hochfahrens des Systems ausführen. Bei Block **1002** kann das Client-Computersystem auf normale Weise hochgefahren werden und ein Vorrichtungstreiber **526** für die Vorrichtung kann in den Hauptspeicher geladen werden. Wenn der Vorrichtungstreiber initialisiert wird und mit der Ausführung beginnt, bestimmt der Vorrichtungstreiber bei Block **1004**, ob in der Massenspeichervorrichtung **308** für die Vorrichtung **506** bereits ein verschlüsseltes lokalisiertes Schlüssel-Blob **524** gespeichert ist. Falls ja, muß keine weitere Aufbauverarbeitung ausgeführt werden und die Aufbauverarbeitung endet bei Block **1006**. Falls nicht, geht die Verarbeitung in Block **1008** weiter. In Block **1008** veranlasst der Vorrichtungstreiber die Anzeige einer Nachricht für den Benutzer des Client-Computersystems, in der dieser zum Einlegen der Verteilungs-CD **522** aufgefordert wird. Sobald die CD von dem Computersystem gelesen wird, startet der Vorrichtungstreiber das Schlüsselabruf-Utility-Softwaremodul (in Fig. 5 nicht dargestellt), das auf der CD gespeichert ist. Die Schlüsselabruf-Utility fragt die Vorrichtung nach ihrer Gruppen-ID, die der Streuwert des öffentlichen Gruppenschlüssels Gpub sein kann, und nach der Gruppenzahl **509**. Die Vorrichtung sendet diese Werte zurück, welche die Utility benutzt, um das richtig signierte Gruppenverzeichnis aus der Schlüssel-Blob-Datenbank auf der CD zu finden. Diese Utility erteilt der Vorrichtung **506** auch einen Schlüsselerfassungsbefehl, um den Prozeß zur Erfassung eines privaten DP-Schlüssels der Vorrichtung zu initiieren.

[0055] Daraufhin benutzt die Vorrichtung in Block **1010** ihre Einwegfunktion f, um den symmetrischen Schlüssel SKEY (nun zur Verwendung bei der Entschlüsselung) aus dem eingebetteten RAND-Wert **508** (SKEY = f(RAND)) erneut zu erzeugen. Bei Block **1012** erzeugt die Vorrichtung dann ihr eindeutiges Vorrichtungs-ID-Etikett, indem sie den SKEY zum Verschlüsseln eines "Nulleintrags" (zum Beispiel einer kleinen Anzahl von Nullbytes) (Vorrichtung-ID = Verschlüsseln (0..0) mit Hilfe des SKEY) benutzt. In einer Ausführungsform der vorliegenden Erfindung kann keiner dieser Werte außerhalb der Vorrichtung enthüllt werden. Die Vorrichtung signalisiert dann ihre Bereitschaft zum Fortschreiten.

[0056] Bei Block **1014** durchsucht die Schlüsselabruf-Utility die Schlüssel-Blob-Datenbank **520** auf der CD nach dem Gruppenverzeichnis, das die passende Gruppenzahl enthält, extrahiert das Gruppenverzeichnis und transferiert das gesamte Gruppenverzeichnis an die Vorrichtung.

[0057] Bei Block **1016** analysiert die Vorrichtung das gesamte gelieferte Gruppenverzeichnis syntaktisch, bewahrt jedoch nur die Gruppenzahl, den Streuwert des Gruppenverzeichnisses, den öffentlichen Gruppenschlüssel Gpub und das erste Feld <Device ID, Encrypted Keyblob>, das mit der eigenen Vorrichtungs-ID der Vorrichtung (die in Block **1012** erzeugt wird) übereinstimmt. Bei Block **1018** verifiziert die Vorrichtung nun das Gruppenverzeichnis. In einer Ausführungsform vergleicht die Vorrichtung das extrahierte Gruppennummernfeld mit der Gruppenzahl, die in der Vorrichtung eingebettet ist. Wenn sie nicht übereinstimmen, kann der Schlüsselerfassungsprozeß beendet werden. Falls nicht, hashed die Vorrichtung das extrahierte Gpub-Feld und vergleicht es mit dem Gpub-Hash in der Vorrichtung. Wenn die Hashes nicht übereinstimmen, kann der Schlüsselerfassungsprozeß beendet werden. Falls nicht, benutzt die Vorrichtung den validierten Gpub-Schlüssel, um die bereitgestellte Signatur auf dem Streuwert des

Gruppenverzeichnisses zu verifizieren. Wenn die Signatur verifiziert ist, ist das Gruppenverzeichnis verifiziert und der Prozeß geht in Block **1120** von Fig. 11 weiter.

[0058] Wenn in einer Ausführungsform eine Rogue-Software versucht, einen Schlüsselerfassungsbefehl an die Vorrichtung zu senden, nachdem die Vorrichtung das Schlüssel-Blob hat, antwortet die Vorrichtung nicht auf die Rogue-Software mit der Gruppenzahl. Statt dessen antwortet die Vorrichtung mit einer Fehleranzeige. Wenn die Vorrichtung Zugang zu einem lokalisierten Schlüssel-Blob hat, dann wird die Funktionalität des Schlüsselerfassungsbefehls in der Tat deaktiviert. Folglich enthüllt die Vorrichtung die Gruppenzahl nicht, außer wenn sie das Schlüssel-Blob nicht aufweist.

[0059] Bei Block **1120** entschlüsselt die Vorrichtung das verschlüsselte Schlüssel-Blob mit Hilfe des symmetrischen Schlüssels SKEY, um DPpri und den DPpri-Digest zu liefern, und speichert diese Werte in ihrem nichtflüchtigen Speicher (Entschlüsseltes Schlüssel-Blob = Entschlüsseln (IV, DPpri, DPpri-Digest mittels SKEY). Der Initialisierungsvektor (IV) kann verworfen werden. Bei Block **1122** überprüft die Vorrichtung dann die Integrität des DPpri durch Hashen des DPpri und Vergleichen des Ergebnisses mit dem DPpri-Digest. Wenn der Vergleich positiv ist, akzeptiert die Vorrichtung DPpri als ihren gültigen Schlüssel. Die Vorrichtung kann auch ein Schlüssel-Erfaßt-Flag als wahr setzen, um anzuzeigen, daß der private DP-Schlüssel erfolgreich erfaßt worden ist. Bei Block **1124** wählt die Vorrichtung einen neuen IV und erzeugt ein neues verschlüsseltes lokalisiertes Schlüssel-Blob mit Hilfe des neuen IV (Lokalisiertes Schlüssel-Blob = Verschlüsseln (IV2, DPpri, DPpri-Digest) mittels SKEY). Das neue verschlüsselte lokalisierte Schlüssel-Blob kann zur Schlüsselabruf-Utility zurückgesendet werden. Bei Block **1126** speichert die Schlüsselabruf-Utility das verschlüsselte, lokalisierte Schlüssel-Blob in dem Speicher innerhalb des Client-Computersystems (wie zum Beispiel einer Massenspeichervorrichtung **308**). Der DPpri der Vorrichtung wird nun in dem Client-Computersystem sicher gespeichert.

[0060] Sobald die Vorrichtung den DPpri während der Aufbauverarbeitung erfaßt hat, kann die Vorrichtung den DPpri benutzen. Fig. 12 ist ein Flußdiagramm, das die Verarbeitung eines Client-Computersystems gemäß einer Ausführungsform der vorliegenden Erfindung darstellt. Das Client-Computersystem kann diese Handlungen zu jeder Zeit nach Abschluß des Setups ausführen. Bei Block **1202** kann das Client-Computersystem normal hochgefahren werden und ein Vorrichtungstreiber **526** für die Vorrichtung kann in den Hauptspeicher geladen werden. Wenn der Vorrichtungstreiber gestartet wird und mit der Ausführung beginnt, bestimmt der Vorrichtungstreiber, ob in der Massenspeichervorrichtung **308** für die Vorrichtung **506** bereits ein verschlüsseltes lokalisiertes Schlüssel-Blob **524** gespeichert ist. Falls nicht, wird die Setup-Verarbeitung aus Fig. 10 und Fig. 11 ausgeführt. Wenn ein verschlüsseltes lokalisiertes Schlüssel-Blob für diese Vorrichtung verfügbar ist, geht die Verarbeitung in Block **1206** weiter. Bei Block **1206** ruft der Vorrichtungstreiber das verschlüsselte lokalisierte Schlüssel-Blob ab und transferiert das Schlüssel-Blob an die Vorrichtung. In einer Ausführungsform kann der Transfer des Schlüssel-Blobs durch Ausführen eines Schlüssel-Blob-Ladebefehls erreicht werden.

[0061] Die Vorrichtung benutzt in Block **1208** ihre Einwegfunktion f, um den symmetrischen Schlüssel SKEY (nun zur Verwendung bei der Entschlüsselung) aus dem eingebetteten RAND-Wert **508** (SKEY = f(RAND)) erneut zu erzeugen. Bei Block **1210** entschlüsselt die Vorrichtung das verschlüsselte Schlüssel-Blob mit Hilfe des symmetrischen Schlüssels SKEY, um DPpri und den DPpri-Digest zu liefern, und speichert diese Werte in ihrem nichtflüchtigen Speicher (Entschlüsseltes Schlüssel-Blob = Entschlüsseln (IV, DPpri, DPpri-Digest mittels SKEY). Der zweite Initialisierungsvektor (IV2) kann verworfen werden. Bei Block **1212** überprüft die Vorrichtung dann die Integrität von DPpri durch Hashen von DPpri und Vergleichen des Ergebnisses mit dem DPpri-Digest. Wenn der Vergleich positiv ist (zum Beispiel die Digests übereinstimmen), akzeptiert die Vorrichtung den DPpri als den vorher erfaßten gültigen Schlüssel und aktiviert ihn zur Benutzung. Die Vorrichtung kann auch ein Schlüssel-Erfaßt-Flag als wahr setzen, um anzuzeigen, daß der private DP-Schlüssel erfolgreich erfaßt worden ist. Bei Block **1214** wählt die Vorrichtung wieder einen anderen IV und erzeugt ein neues verschlüsseltes lokalisiertes Schlüssel-Blob mit Hilfe des neuen IV (Lokalisiertes Schlüssel-Blob = Verschlüsseln (IV3, DPpri, DPpri-Digest) mittels SKEY). Das neue verschlüsselte lokalisierte Schlüssel-Blob kann zur Schlüsselabruf-Utility zurückgesendet werden. Bei Block **1216** speichert die Schlüsselabruf-Utility das verschlüsselte, lokalisierte Schlüssel-Blob in dem Speicher innerhalb des Client-Computersystems (wie zum Beispiel einer Massenspeichervorrichtung **308**). Der DPpri der Vorrichtung wird nun erneut in dem Client-Computersystem sicher gespeichert.

[0062] In einer Ausführungsform der vorliegenden Erfindung ist es nicht notwenig, alle privaten DP-Schlüssel der Vorrichtung für die signierten Gruppen auf einmal zu erzeugen. Unter der Annahme, daß die Verteilungs-CD regelmäßig aktualisiert wird, könnten die privaten DP-Schlüssel der Vorrichtung je nach Bedarf in Bündeln erzeugt werden. Immer wenn die Verteilungs-CD „gebrannt" wird, enthält sie die signierten Gruppen für die Schlüssel-Blob-Datenbank, die bisher erzeugt worden ist, einschließlich derjeni-

gen Vorrichtungsschlüssel, die erzeugt, jedoch den Vorrichtungen noch nicht zugewiesen worden sind.

[0063] Wenn das gesamte Gruppenverzeichnis in einer Ausführungsform in Block **1018** aus Fig. 10 verarbeitet wird, kann die Vorrichtung im Falle einer Fehlererkennung ein Flag setzen, das anzeigt, daß der Fehler aufgetreten ist, sollte jedoch mit der Verarbeitung fortfahren. Wenn alle Schritte für den System-Setup vollendet worden sind, kann die Vorrichtung dem Vorrichtungstreiber den Fehler signalisieren. Dies kann einen Angreifer daran hindern, Information aus der Art und dem Ort des Fehlers zu erhalten.

[0064] In einer Ausführungsform können die hierin beschriebenen Verfahren etwa 40 Byte an nichtflüchtigem Speicher in der Vorrichtung benutzen. In einer anderen Ausführungsform kann dieser auf etwa 20 Byte reduziert werden, wenn der Gpub-Schlüssel-Hash in dem verschlüsselten Schlüssel-Blob der Vorrichtung enthalten und nicht in dem nichtflüchtigen Speicher auf der Vorrichtung gespeichert ist. Wenn die Vorrichtung das verschlüsselte Schlüssel-Blob entschlüsselt, kann die Vorrichtung in diesem Fall den Gpub-Hash abrufen, den Hash zum Überprüfen des Gpub-Schlüssels benutzen und den Gpub-Schlüssel zum Überprüfen der Signatur auf dem gesamten Gruppenverzeichnis benutzen.

[0065] Obwohl die hierin erläuterten Vorgänge als ein sequentieller Prozeß beschrieben werden können, können einige der Vorgänge in der Tat parallel oder gleichzeitig ausgeführt werden. Außerdem kann die Reihenfolge der Vorgänge in einigen Ausführungsformen neu angeordnet werden, ohne von dem Geist der Erfindung abzuweichen.

[0066] Die hierin beschriebenen Techniken sind nicht auf eine bestimmte Hardware- oder Softwarekonfiguration eingeschränkt; sie können in jeder beliebigen Rechen- oder Verarbeitungsumgebung Anwendung finden. Die Techniken können in Hardware, Software oder einer Kombination der beiden umgesetzt werden. Die Techniken können in Programmen, die auf programmierbaren Maschinen wie mobilen oder stationären Computern, persönlichen digitalen Assistenten, Set-Top-Boxes, Mobiltelefonen und Funkrufempfängern und anderen elektronischen Vorrichtungen ausgeführt werden, die jeweils einen Prozessor, ein Speichermedium, das von dem Prozessor gelesen werden kann (einschließlich eines flüchtigen und nichtflüchtigen Speichers und/oder Speicherelementen), mindestens eine Eingabevorrichtung und eine oder mehrere Ausgabevorrichtungen aufweisen. Ein Programmcode wird auf die Daten angewendet, die mit Hilfe der Eingabevorrichtung eingegeben werden, um die beschriebenen Funktionen auszuführen und Ausgabeinformation zu erzeugen. Die Ausgabeinformation kann auf eine oder mehrere Ausgabevorrichtungen angewendet werden. Der Durchschnittsfachmann versteht, daß die Erfindung mit verschiedenen Computersystemkonfigurationen umgesetzt werden kann, einschließlich Mehrprozessorsystemen, Minicomputern, Großrechnern und dergleichen. Die Erfindung kann auch in verteilten Rechenumgebungen umgesetzt werden, in denen Befehle von entfernten Verarbeitungsvorrichtungen ausgeführt werden, die durch ein Kommunikationsnetzwerk verbunden sind.

[0067] Jedes Programm kann in einer verfahrensorientierten oder Objekt-orientierten Programmiersprache auf hoher Ebene ausgeführt werden, um mit einem Verarbeitungssystem zu kommunizieren. Die Programme können jedoch je nach Wunsch in Assemblersprache oder Maschinensprache ausgeführt werden. In jedem Fall kann die Sprache kompiliert oder interpretiert werden.

[0068] Programmbefehle können benutzt werden, um zu bewirken, daß ein Universal- oder Spezialverarbeitungssystem, das mit den Befehlen programmiert ist, die hierin beschriebenen Vorgänge ausführt. Als Alternative können die Vorgänge durch spezifische Hardwarekomponenten ausgeführt werden, die eine festverdrahtete Logik zum Ausführen von Vorgängen enthalten, oder durch jede beliebige Kombination von programmierten Computerkomponenten und kundenspezifischen Hardwarekomponenten. Die hierin beschriebenen Verfahren können als ein Computerprogrammprodukt bereitgestellt werden, das ein maschinenlesbares Medium aufweisen kann, auf dem Befehle gespeichert sind, die zum Programmieren eines Verarbeitungssystems oder einer anderen elektronischen Vorrichtung zur Ausführung der Verfahren benutzt werden können. Der hierin verwendete Ausdruck "maschinenlesbares Medium" soll jedes Medium einschließen, das eine Sequenz von Befehlen zur Ausführung durch die Maschine speichern oder verschlüsseln und bewirken kann, daß die Maschine jedes der hierin beschriebenen Verfahren ausführt. Der Ausdruck "maschinenlesbares Medium" soll dementsprechend einschließen, jedoch nicht beschränkt sein auf Festspeicher, optische und magnetische Platten und eine Trägerwelle, die ein Datensignal verschlüsselt. Darüber hinaus wird im Stand der Technik im allgemeinen von einer Software in der einen oder anderen Form (zum Beispiel Programm, Prozedur, Prozeß, Anwendung, Modul, Logik und so weiter) gesprochen, wenn diese eine Handlung ausführt oder ein Ergebnis bewirkt. Solche Ausdrücke sind lediglich eine Kurzform zur Bezeichnung dessen, daß die Ausführung der Software von einem Verarbeitungssystem bewirkt, daß der Prozessor eine Handlung ausführt oder ein Ergebnis hervorbringt.

[0069] Wenngleich diese Erfindung mit Bezug auf die beispielhaften Ausführungsformen beschrieben

worden ist, soll diese Beschreibung nicht in einschränkendem Sinne verstanden werden. Verschiedene Modifikationen der beispielhaften Ausführungsformen sowie andere Ausführungsformen der Erfindung, die für den Fachmann des Gebiets, zu dem die Erfindung gehört, offensichtlich sind, gelten als innerhalb des Geistes und des Schutzbereichs der Erfindung liegend.

ZUSAMMENFASSUNG

[0070] Das Bereitstellen eines privaten Direktbeweis-Schlüssels in einer signierten Gruppe von Schlüsseln für eine Vorrichtung, die in einem Client-Computersystem in dem Feld kann sicher erreicht werden, ohne eine bedeutende nichtflüchtige Speicherung in der Vorrichtung zu erfordern. Ein einmaliger pseudo-zufälliger Wert wird erzeugt und bei der Herstellung zusammen mit einer Gruppenzahl in der Vorrichtung gespeichert. Der pseudo-zufällige Wert wird benutzt, um einen symmetrischen Schlüssel zum Verschlüsseln einer Datenstruktur zu erzeugen, die einen privaten Direktbeweis-Schlüssel und einen privaten Schlüssel-Digest aufweist, die mit der Vorrichtung assoziiert ist. Die resultierende verschlüsselte Datenstruktur wird in einer signierten Gruppe von Schlüsseln (zum Beispiel einem signierten Gruppenverzeichnis) auf einem entfernbaren Speichermedium (wie einer CD oder DVD) gespeichert und an den Besitzer des Client-Computersystems verteilt. Wenn die Vorrichtung auf dem Client-Computersystem gestartet wird, überprüft das System, ob eine lokalisierte verschlüsselte Datenstruktur in dem System vorhanden ist. Falls nicht, erhält das System das assoziierte signierte Gruppenverzeichnis der verschlüsselten Datenstrukturen von dem entfernbaren Speichermedium und verifiziert das signierte Gruppenverzeichnis. Die Vorrichtung entschlüsselt die verschlüsselte Datenstruktur mit Hilfe eines symmetrischen Schlüssels, der aus seinem gespeicherten pseudo-zufälligen Wert neu erstellt wird, um den privaten Direktbeweis-Schlüssel zu erhalten, wenn das Gruppenverzeichnis gültig ist. Wenn der private Schlüssel gültig ist, kann er zur nachfolgenden Authentifizierungsverarbeitung von der Vorrichtung in dem Client-Computersystem benutzt werden.

Patentansprüche

1. Verfahren, umfassend:
Erzeugen einer verschlüsselten Datenstruktur, die mit einer Vorrichtung assoziiert ist, wobei die verschlüsselte Datenstruktur einen privaten Schlüssel und ein privates Schlüssel-Digest umfaßt;
Erzeugen eines Identifikators, der auf einem pseudo-zufällig erzeugten Wert beruht, für die verschlüsselte Datenstruktur;
Speichern des Identifikators und der verschlüsselten Datenstruktur in einem signierten Gruppenverzeichnis auf einem entfernbaren Speichermedium; und
Speichern des pseudo-zufälligen Wertes und einer Gruppenzahl, die dem signierten Gruppenverzeichnis entspricht, in einem nichtflüchtigen Speicher innerhalb der Vorrichtung.

2. Verfahren nach Anspruch 1, ferner umfassend das Verteilen des entfernbaren Speichermediums und der Vorrichtung.

3. Verfahren nach Anspruch 1, ferner umfassend das Erzeugen eines Direktbeweis-Familienschlüsselpaars für eine Klasse von Vorrichtungen.

4. Verfahren nach Anspruch 1, ferner umfassend das Erzeugen eines Schlüsselpaars zum Signieren und Verifizieren des Gruppenverzeichnisses.

5. Verfahren nach Anspruch 4, ferner umfassend das Speichern eines Hashs des öffentlichen Schlüssels des Gruppenverzeichnis-Schlüsselpaars in einem nichtflüchtigen Speicher der Vorrichtung.

6. Verfahren nach Anspruch 1, ferner umfassend das Auswählen einer Gruppengröße für das signierte Gruppenverzeichnis.

7. Verfahren nach Anspruch 3, wobei der private Schlüssel einen privaten Direktbeweis-Schlüssel umfaßt, der mit einem öffentlichen Schlüssel des Direktbeweis-Familienschlüsselpaars assoziiert ist, und ferner umfassend das Hashen des privaten Direktbeweis-Schlüssels, um den privaten Schlüssel-Digest zu erzeugen.

8. Verfahren nach Anspruch 1, ferner umfassend das Erzeugen eines symmetrischen Schlüssels, der auf dem pseudo-zufälligen Wert für die Vorrichtung beruht.

9. Verfahren nach Anspruch 8, wobei das Erzeugen des Identifikators das Verschlüsseln eines Datenwertes unter Verwendung des symmetrischen Schlüssels umfaßt.

10. Verfahren nach Anspruch 8, ferner umfassend das Verschlüsseln der Datenstruktur unter Verwendung des symmetrischen Schlüssels.

11. Verfahren nach Anspruch 1, wobei die verschlüsselte Datenstruktur ferner einen zufälligen Initialisierungsvektor umfaßt.

12. Verfahren nach Anspruch 1, wobei das entfernbare Speichermedium mindestens eine von einer CD oder einer digitalen Videoplatte (DVD) umfaßt.

13. Verfahren nach Anspruch 1, wobei der pseudo-zufällige Wert für die Vorrichtung eindeutig ist.

14. Gegenstand, umfassend: ein erstes Speichermedium mit mehreren maschinenlesbaren Befehlen, wobei, wenn die Befehle von einem Prozessor ausgeführt werden, die Befehle die Lieferung privater Schlüssel in signierten Gruppen an Vorrichtungen bereitstellen, durch
Erzeugen einer verschlüsselten Datenstruktur, die mit einer Vorrichtung assoziiert ist, wobei die verschlüsselte Datenstruktur einen privaten Schlüssel und ein privates Schlüssel-Digest umfaßt;
Erzeugen eines Identifikators, der auf einem pseudo-zufällig erzeugten Wert beruht, für die verschlüsselte Datenstruktur;
Speichern des Identifikators und der verschlüsselten Datenstruktur in einem signierten Gruppenverzeichnis auf einem entfernbaren Speichermedium; und
Bewirken des Speicherns des pseudo-zufälligen Wertes und einer Gruppenzahl, die dem signierten Gruppenverzeichnis entspricht, in einen nichtflüchtigen Speicher innerhalb der Vorrichtung.

15. Gegenstand nach Anspruch 14, ferner umfassend Befehle zum Erzeugen eines Schlüsselpaars zum Signieren und Verifizieren des Gruppenverzeichnisses.

16. Gegenstand nach Anspruch 15, ferner umfassend Befehle zum Speichern eines Hashes des öffentlichen Schlüssels des Gruppenverzeichnis-Schlüsselpaars in einen nichtflüchtigen Speicher der Vorrichtung.

17. Gegenstand nach Anspruch 14, ferner umfassend Befehle zum Auswählen einer Gruppengröße für das signierte Gruppenverzeichnis.

18. Gegenstand nach Anspruch 14, ferner umfassend Befehle zum Erzeugen eines Direktbeweis-Familienschlüsselpaars für eine Klasse von Vorrichtungen.

19. Gegenstand nach Anspruch 14, wobei der private Schlüssel einen privaten Direktbeweis-Schlüssel umfaßt, der mit einem öffentlichen Schlüssel des Direktbeweis-Familienschlüsselpaars assoziiert ist, und ferner umfassend Befehle zum Hashen des privaten Direktbeweis-Schlüssels, um den privaten Schlüssel-Digest zu erzeugen.

20. Gegenstand nach Anspruch 14, ferner umfassend Befehle zum Erzeugen eines symmetrischen Schlüssels, der auf dem pseudo-zufälligen Wert für die Vorrichtung beruht.

21. Gegenstand nach Anspruch 20, wobei Befehle zum Erzeugen des Identifikators Befehle zum Verschlüsseln eines Datenwertes unter Verwendung des symmetrischen Schlüssels umfassen.

22. Gegenstand nach Anspruch 20, ferner umfassend Befehle zum Verschlüsseln der Datenstruktur mit Hilfe des symmetrischen Schlüssels.

23. Gegenstand nach Anspruch 14, wobei die verschlüsselte Datenstruktur ferner einen zufälligen Initialisierungsvektor umfaßt.

24. Gegenstand nach Anspruch 14, wobei der pseudo-zufällige Wert für die Vorrichtung einmalig ist.

25. Verfahren, umfassend:
Bestimmen, ob eine verschlüsselte Datenstruktur, die einen privaten Schlüssel und ein privates Schlüssel-Digest umfaßt, die mit einer Vorrichtung assoziiert ist, die in einem Computersystem installiert ist, in einem Speicher auf dem Computersystem gespeichert wird; und
wenn die verschlüsselte Datenstruktur nicht gespeichert wird, Erhalten der verschlüsselten Datenstruktur, die mit der Vorrichtung assoziiert ist, in einem signierten Gruppenverzeichnis von einem entfernbaren Speichermedium, auf das das Computersystem zugreifen kann, wobei das entfernbare Speichermedium eine Datenbank von signierten Gruppenverzeichnissen speichert.

26. Verfahren nach Anspruch 25, wobei das entfernbare Speichermedium mindestens eines von einer CD oder einer digitalen Videoplatte (DVD) umfaßt, die von einem Hersteller der Vorrichtung erzeugt wird.

27. Verfahren nach Anspruch 25, wobei das Erhalten der verschlüsselten Datenstruktur das Erteilen des Schlüsselerfassungsbefehls an die Vorrichtung zum Initiieren eines privaten Schlüsselerfassungsprozesses umfaßt.

28. Verfahren nach Anspruch 25, wobei der private Schlüssel einen privaten Direktbeweis-Schlüssel umfaßt, der mit einem öffentlichen Schlüssel eines Direktbeweis-Familienschlüsselpaars für eine Klasse von Vorrichtungen assoziiert ist.

29. Verfahren nach Anspruch 27, wobei der Prozeß zur Erfassung des privaten Schlüssels das Erzeugen eines symmetrischen Schlüssels umfaßt, der auf einem einmaligen pseudozufälligen Wert basiert, der in der Vorrichtung gespeichert ist.

30. Verfahren nach Anspruch 29, wobei der Prozeß zur Erfassung des privaten Schlüssels das Erzeugen eines Vorrichtungsidentifikators, der auf dem pseudo-zufälligen Wert basiert, für die verschlüsselte Datenstruktur umfaßt.

31. Verfahren nach Anspruch 27, wobei der Prozeß zur Erfassung des privaten Schlüssels das Erhalten des signierten Gruppenverzeichnisses aus dem entfernbaren Speichermedium umfaßt, entsprechend

einer Gruppenzahl der Vorrichtung.

32. Verfahren nach Anspruch 30, ferner umfassend das syntaktische Analysieren des signierten Gruppenverzeichnisses, um eine Gruppenzahl, einen öffentlichen Gruppenschlüssel und die verschlüsselte Datenstruktur, die dem Vorrichtungsidentifikator entspricht, zu erhalten.

33. Verfahren nach Anspruch 31, ferner umfassend das Verifizieren des signierten Gruppenverzeichnisses.

34. Verfahren nach Anspruch 32, wobei der Prozeß zur Erfassung des privaten Schlüssels ferner das Entschlüsseln der verschlüsselten Datenstruktur umfaßt, die von dem entfernbaren Speichermedium unter Verwendung des symmetrischen Schlüssels empfangen wird, um den privaten Schlüssel und den privaten Schlüssel-Digest zu erhalten.

35. Verfahren nach Anspruch 34, wobei der Prozeß zur Erfassung des privaten Schlüssels ferner das Hashen des privaten Schlüssels, um einen neuen privaten Schlüssel-Digest zu erzeugen, das Vergleichen des privaten Schlüssel-Digest aus der entschlüsselten Datenstruktur mit dem neuen privaten Schlüssel-Digest und das Akzeptieren des privaten Schlüssels als gültig für die Vorrichtung umfaßt, wenn die Digests übereinstimmen.

36. Gegenstand, umfassend: ein erstes Speichermedium mit mehreren maschinenlesbaren Befehlen, wobei, wenn die Befehle von einem Prozessor ausgeführt werden, die Befehle für den Erhalt eines privaten Schlüssels aus einem signierten Gruppenverzeichnis für eine Vorrichtung sorgen, die in einem Computersystem installiert ist, durch
Bestimmen, ob eine verschlüsselte Datenstruktur, die einen privaten Schlüssel und ein privates Schlüssel-Digest umfaßt, die mit einer Vorrichtung assoziiert ist, die in einem Computersystem installiert ist, in einem Speicher auf dem Computersystem (**904**) gespeichert ist; und
wenn die verschlüsselte Datenstruktur nicht gespeichert ist, Erhalten der verschlüsselten Datenstruktur, die mit der Vorrichtung assoziiert ist, in einem signierten Gruppenverzeichnis von einem entfernbaren Speichermedium, auf das das Computersystem zugreifen kann, wobei das entfernbare Speichermedium eine Datenbank von signierten Gruppenverzeichnissen speichert.

37. Gegenstand nach Anspruch 36, wobei Befehle zum Erhalten der verschlüsselten Datenstruktur Befehle zum Erteilen des Schlüsselerfassungsbefehls an die Vorrichtung zum Initiieren eines Prozesses zur Erfassung des privaten Schlüssels umfassen.

38. Gegenstand nach Anspruch 36, wobei der private Schlüssel einen privaten Direktbeweis-Schlüssel umfaßt, der mit einem öffentlichen Schlüssel eines Direktbeweis-Familienschlüsselpaars für eine Klasse von Vorrichtungen assoziiert ist.

39. Gegenstand nach Anspruch 37, wobei der Prozeß zur Erfassung des privaten Schlüssels das Erzeugen eines symmetrischen Schlüssels umfaßt, der auf einem einmaligen pseudozufälligen Wert basiert, der in der Vorrichtung gespeichert ist.

40. Gegenstand nach Anspruch 37, wobei der Prozeß zur Erfassung des privaten Schlüssels das Erzeugen eines Vorrichtungsidentifikators, der auf dem pseudo-zufälligen Wert basiert, für die verschlüsselte Datenstruktur umfaßt.

41. Gegenstand nach Anspruch 37, wobei der Prozeß zur Erfassung des privaten Schlüssels das Erhalten des signierten Gruppenverzeichnisses aus dem entfernbaren Speichermedium umfaßt, entsprechend einer Gruppenzahl der Vorrichtung.

42. Gegenstand nach Anspruch 40, ferner umfassend das syntaktische Analysieren des signierten Gruppenverzeichnisses, um eine Gruppenzahl, einen öffentlichen Gruppenschlüssel und die verschlüsselte Datenstruktur, die dem Vorrichtungsidentifikator entspricht, zu erhalten.

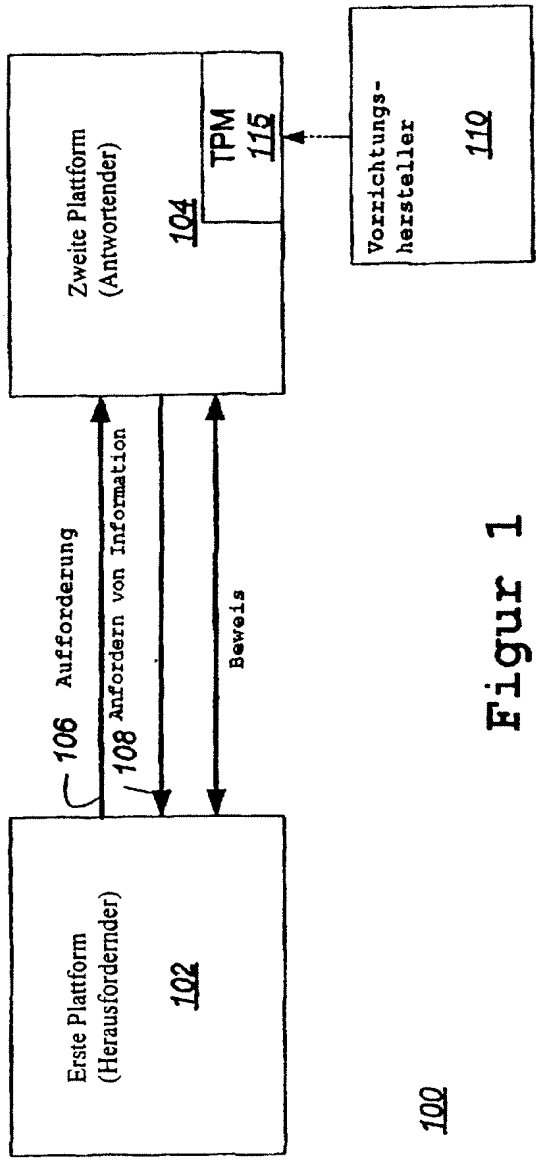
43. Gegenstand nach Anspruch 41, ferner umfassend das Verifizieren des signierten Gruppenverzeichnisses.

44. Gegenstand nach Anspruch 42, wobei der Prozeß zur Erfassung des privaten Schlüssels ferner das Entschlüsseln der verschlüsselten Datenstruktur umfaßt, die von dem entfernbaren Speichermedium unter Verwendung des symmetrischen Schlüssels empfangen wird, um den privaten Schlüssel und den privaten Schlüssel-Digest zu erhalten.

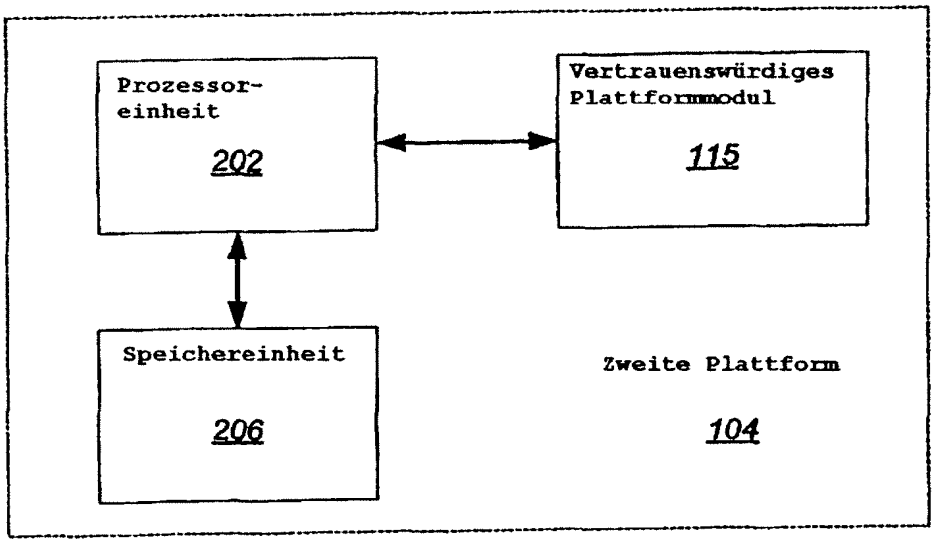
45. Verfahren nach Anspruch 44, wobei der Prozeß zur Erfassung des privaten Schlüssels ferner das Hashen des privaten Schlüssels, um einen neuen privaten Schlüssel-Digest zu erzeugen, das Vergleichen des privaten Schlüssel-Digest aus der entschlüsselten Datenstruktur mit dem neuen privaten Schlüssel-Digest und das Akzeptieren des privaten Schlüssels als gültig für die Vorrichtung umfaßt, wenn die Digests übereinstimmen.

Es folgen 11 Blatt Zeichnungen

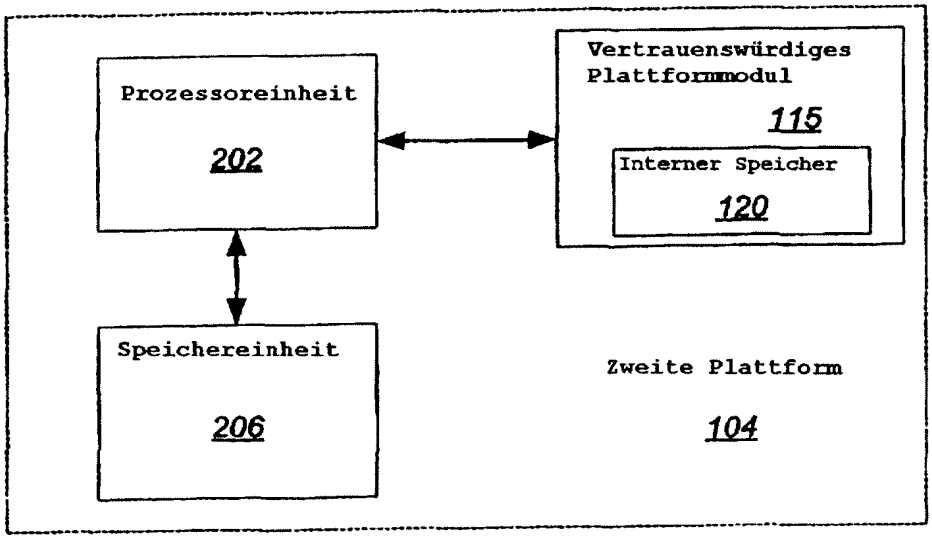
Anhängende Zeichnungen



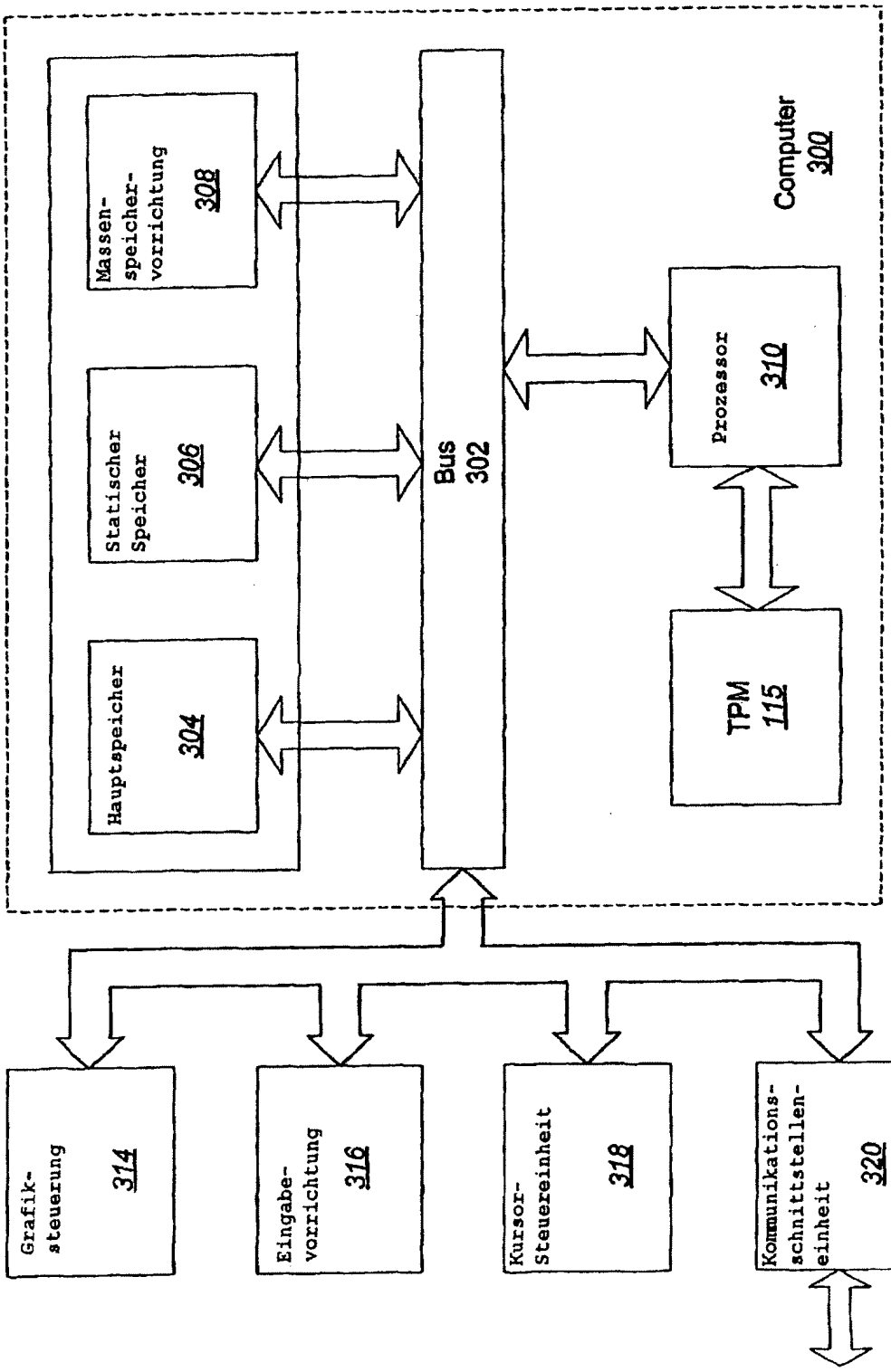
Figur 1



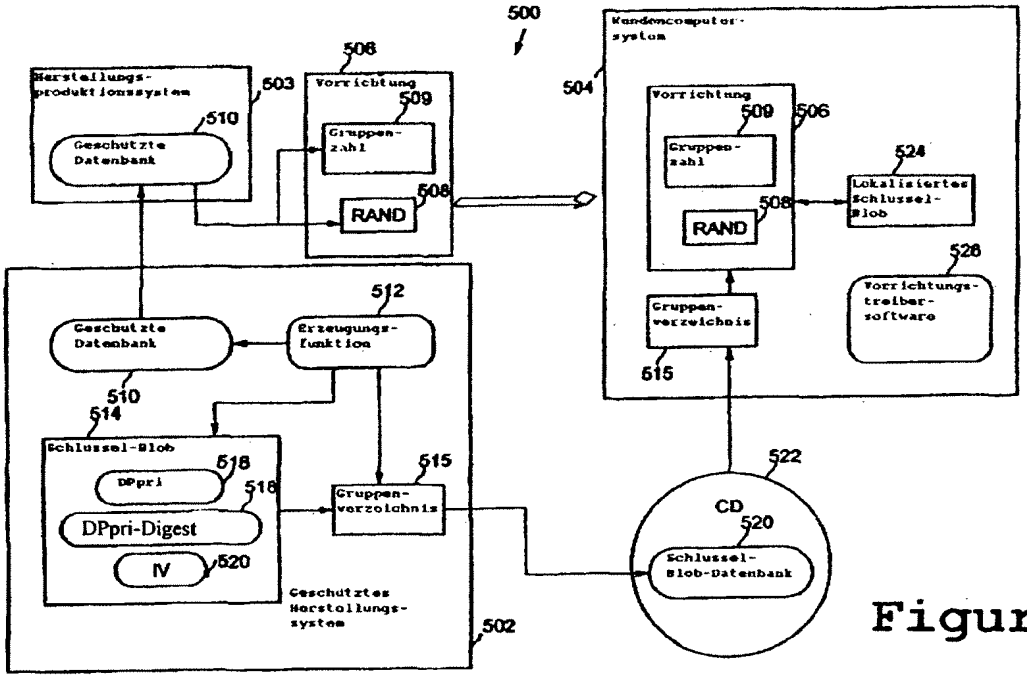
Figur 2



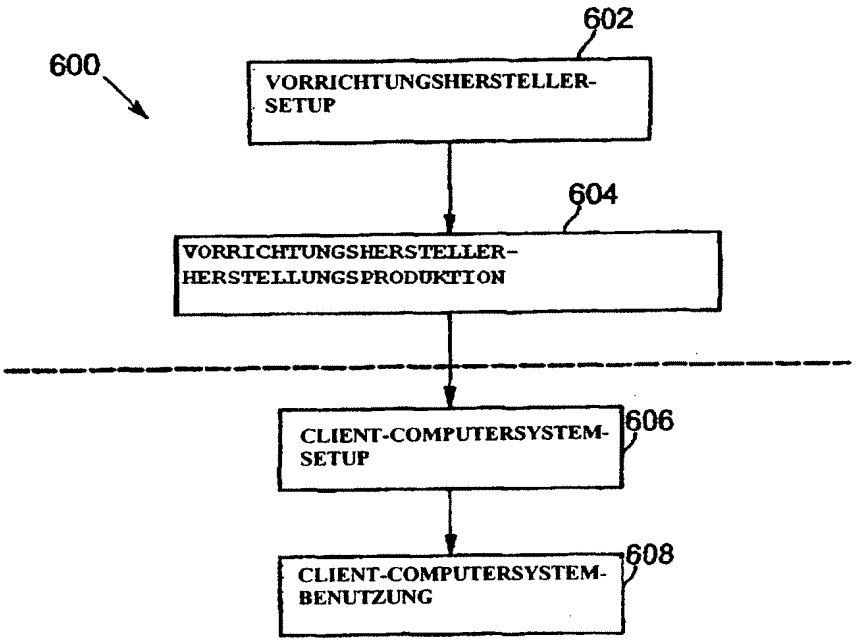
Figur 3


Computer
300
Massen-
speicher-
vorrichtung
308
Statischer
Speicher
306
Hauptspeicher
304
Bus
302
Prozessor
310
TPM
115
104
Grafik-
steuerung
314
Eingabe-
vorrichtung
316
Kursor-
Steuereinheit
318
Kommunikations-
schnittstellen-
einheit
320

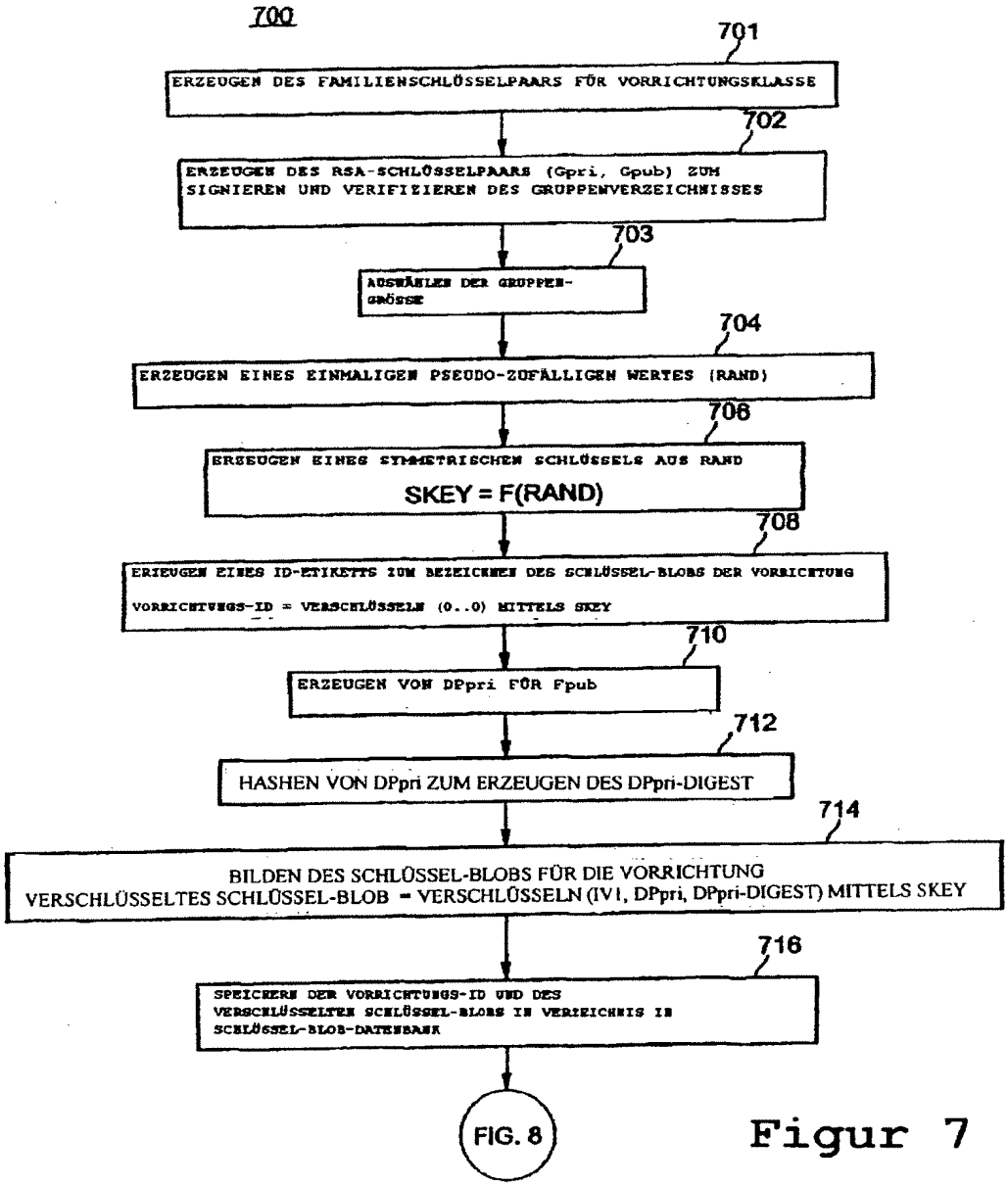
Figur 4


500
Herstellungs-produktionssystem
503
Vorrichtung
506
509
Gruppen-zahl
510
Geschützte Datenbank
508
RAND
Kundencomputer-system
504
Vorrichtung
509
506
Gruppen-zahl
508
RAND
524
Lokalisiertes Schlüssel-Blob
526
Vorrichtungs-treiber-software
Gruppen-verzeichnis
515
512
Geschützte Datenbank
Erzeugungs-funktion
510
514
Schlüssel-Blob
518
DPpri
518
DPpri-Digest
IV
520
515
Gruppen-verzeichnis
522
CD
520
Schlüssel-Blob-Datenbank
Geschütztes Herstellungs-system
502

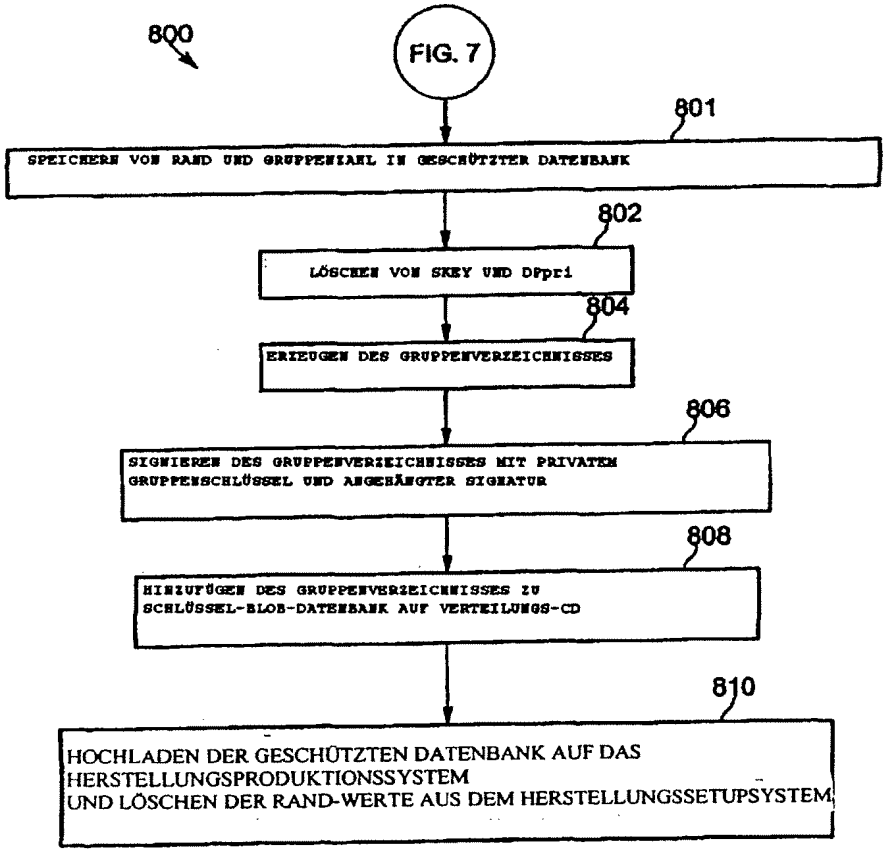
Figur 5


600
602
VORRICHTUNGSHERSTELLER-SETUP
604
VORRICHTUNGSHERSTELLER-HERSTELLUNGSPRODUKTION
CLIENT-COMPUTERSYSTEM-SETUP
606
CLIENT-COMPUTERSYSTEM-BENUTZUNG
608

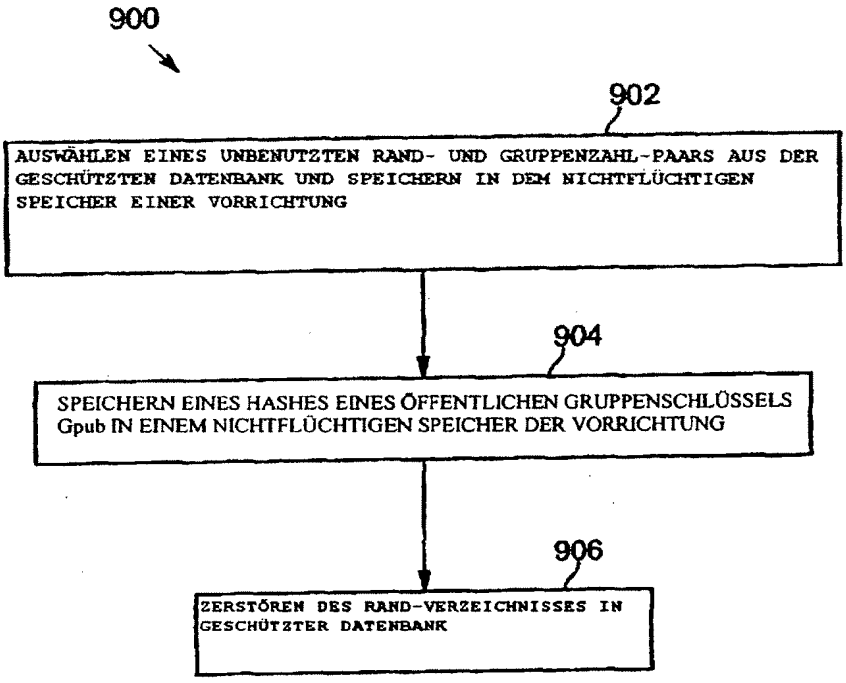
Figur 6


700
701
ERZEUGEN DES FAMILIENSCHLÜSSELPAARS FÜR VORRICHTUNGSKLASSE
702
ERZEUGEN DES RSA-SCHLÜSSELPAARS (Gpri, Gpub) ZUM SIGNIEREN UND VERIFIZIEREN DES GRUPPENVERZEICHNISSES
703
AUSWÄHLEN DER GRUPPEN-GRÖSSE
704
ERZEUGEN EINES EINMALIGEN PSEUDO-ZUFÄLLIGEN WERTES (RAND)
706
ERZEUGEN EINES SYMMETRISCHEN SCHLÜSSELS AUS RAND
SKEY = F(RAND)
708
ERZEUGEN EINES ID-ETIKETTS ZUM BEZEICHNEN DES SCHLÜSSEL-BLOBS DER VORRICHTUNG
VORRICHTUNGS-ID = VERSCHLÜSSELN (0..0) MITTELS SKEY
710
ERZEUGEN VON DPpri FÜR Fpub
712
HASHEN VON DPpri ZUM ERZEUGEN DES DPpri-DIGEST
714
BILDEN DES SCHLÜSSEL-BLOBS FÜR DIE VORRICHTUNG
VERSCHLÜSSELTES SCHLÜSSEL-BLOB = VERSCHLÜSSELN (IV1, DPpri, DPpri-DIGEST) MITTELS SKEY
716
SPEICHERN DER VORRICHTUNGS-ID UND DES VERSCHLÜSSELTEN SCHLÜSSEL-BLOBS IN VERZEICHNIS IN SCHLÜSSEL-BLOB-DATENBANK
FIG. 8

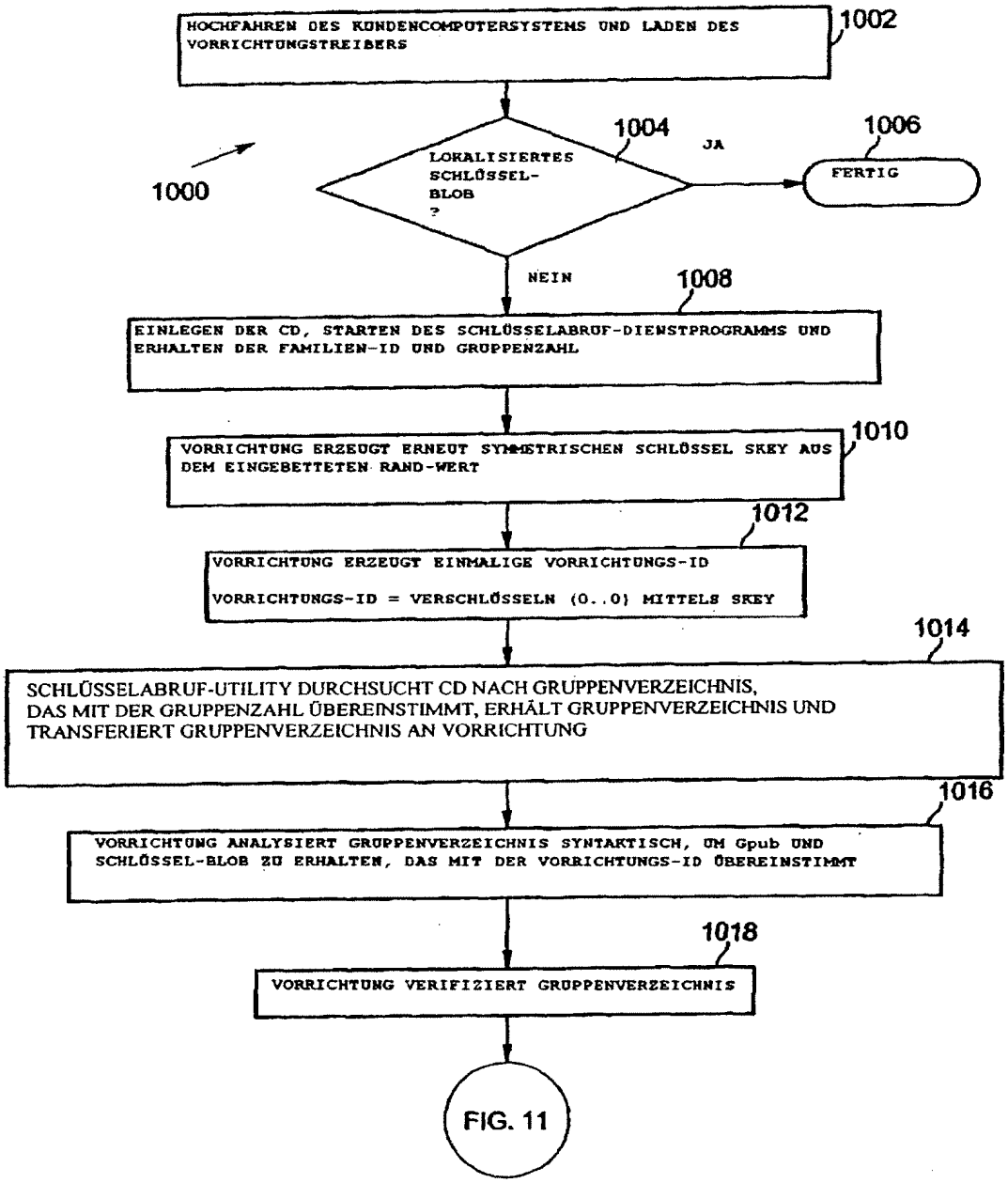
Figur 7


800
FIG. 7
801
SPEICHERN VON RAND UND GRUPPENIAHL IN GESCHÜTZTER DATENBANK
802
LÖSCHEN VON SKEY UND DPpri
804
ERZEUGEN DES GRUPPENVERZEICHNISSES
806
SIGNIEREN DES GRUPPENVERZEICHNISSES MIT PRIVATEN GRUPPENSCHLÜSSEL UND ANGEHÄNGTER SIGNATUR
808
HINZUFÜGEN DES GRUPPENVERZEICHNISSES ZU SCHLÜSSEL-BLOB-DATENBANK AUF VERTEILUNGS-CD
810
HOCHLADEN DER GESCHÜTZTEN DATENBANK AUF DAS HERSTELLUNGSPRODUKTIONSSYSTEM
UND LÖSCHEN DER RAND-WERTE AUS DEM HERSTELLUNGSSETUPSYSTEM

Figur 8


900
902
AUSWÄHLEN EINES UNBENUTZTEN RAND- UND GRUPPENZAHL-PAARS AUS DER GESCHÜTZTEN DATENBANK UND SPEICHERN IN DEM NICHTFLÜCHTIGEN SPEICHER EINER VORRICHTUNG
904
SPEICHERN EINES HASHES EINES ÖFFENTLICHEN GRUPPENSCHLÜSSELS Gpub IN EINEM NICHTFLÜCHTIGEN SPEICHER DER VORRICHTUNG
906
ZERSTÖREN DES RAND-VERZEICHNISSES IN GESCHÜTZTER DATENBANK

Figur 9


HOCHFAHREN DES KUNDENCOMPUTERSYSTEMS UND LADEN DES VORRICHTUNGSTREIBERS
1002
1000
LOKALISIERTES SCHLÜSSEL-BLOB ?
1004
JA
1006
FERTIG
NEIN
1008
EINLEGEN DER CD, STARTEN DES SCHLÜSSELABRUF-DIENSTPROGRAMMS UND ERHALTEN DER FAMILIEN-ID UND GRUPPENZAHL
VORRICHTUNG ERZEUGT ERNEUT SYMMETRISCHEN SCHLÜSSEL SKEY AUS DEM EINGEBETTETEN RAND-WERT
1010
1012
VORRICHTUNG ERZEUGT EINMALIGE VORRICHTUNGS-ID
VORRICHTUNGS-ID = VERSCHLÜSSELN (0..0) MITTELS SKEY
1014
SCHLÜSSELABRUF-UTILITY DURCHSUCHT CD NACH GRUPPENVERZEICHNIS, DAS MIT DER GRUPPENZAHL ÜBEREINSTIMMT, ERHÄLT GRUPPENVERZEICHNIS UND TRANSFERIERT GRUPPENVERZEICHNIS AN VORRICHTUNG
1016
VORRICHTUNG ANALYSIERT GRUPPENVERZEICHNIS SYNTAKTISCH, UM Gpub UND SCHLÜSSEL-BLOB ZU ERHALTEN, DAS MIT DER VORRICHTUNGS-ID ÜBEREINSTIMMT
1018
VORRICHTUNG VERIFIZIERT GRUPPENVERZEICHNIS
FIG. 11

Figur 10

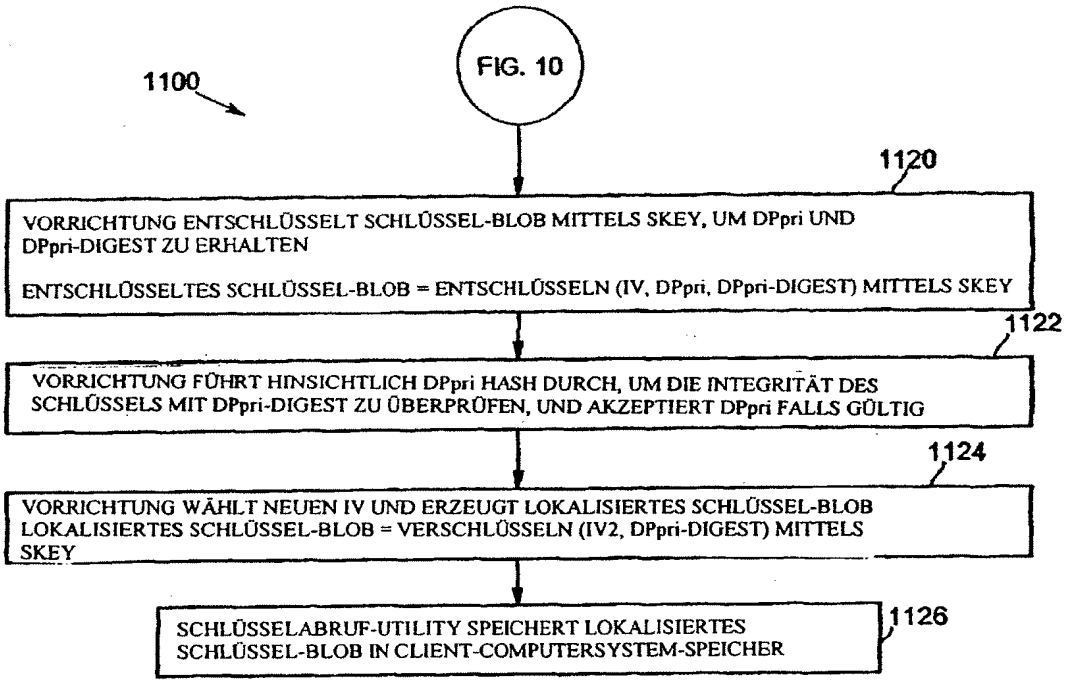
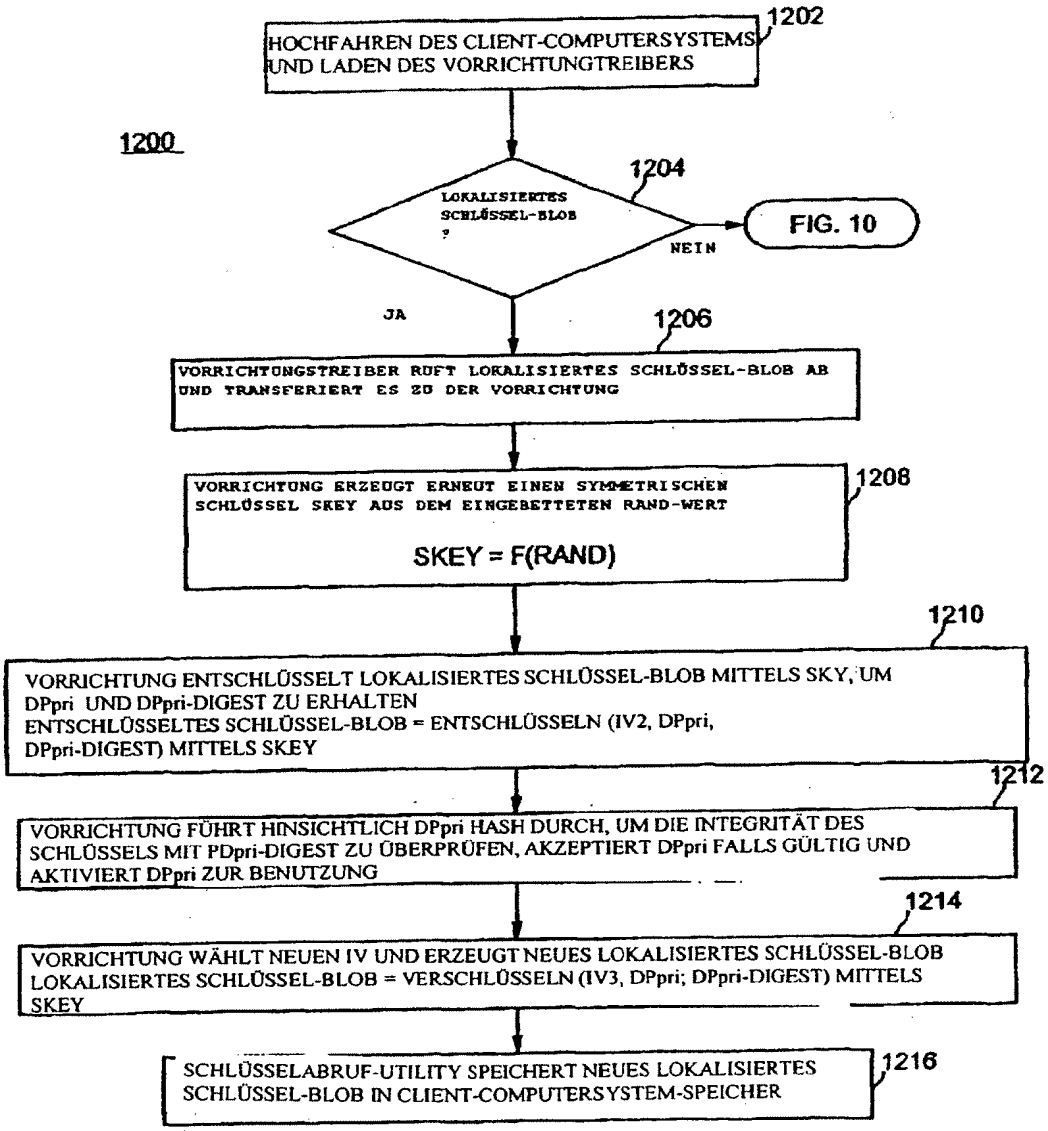


FIG. 10
1100
1120
VORRICHTUNG ENTSCHLÜSSELT SCHLÜSSEL-BLOB MITTELS SKEY, UM DPpri UND DPpri-DIGEST ZU ERHALTEN
ENTSCHLÜSSELTES SCHLÜSSEL-BLOB = ENTSCHLÜSSELN (IV, DPpri, DPpri-DIGEST) MITTELS SKEY
1122
VORRICHTUNG FÜHRT HINSICHTLICH DPpri HASH DURCH, UM DIE INTEGRITÄT DES SCHLÜSSELS MIT DPpri-DIGEST ZU ÜBERPRÜFEN, UND AKZEPTIERT DPpri FALLS GÜLTIG
1124
VORRICHTUNG WÄHLT NEUEN IV UND ERZEUGT LOKALISIERTES SCHLÜSSEL-BLOB
LOKALISIERTES SCHLÜSSEL-BLOB = VERSCHLÜSSELN (IV2, DPpri-DIGEST) MITTELS SKEY
SCHLÜSSELABRUF-UTILITY SPEICHERT LOKALISIERTES SCHLÜSSEL-BLOB IN CLIENT-COMPUTERSYSTEM-SPEICHER
1126

Figur 11


1200
1202
HOCHFAHREN DES CLIENT-COMPUTERSYSTEMS UND LADEN DES VORRICHTUNGTREIBERS
1204
LOKALISIERTES SCHLÜSSEL-BLOB ?
NEIN
FIG. 10
JA
1206
VORRICHTUNGSTREIBER RUFT LOKALISIERTES SCHLÜSSEL-BLOB AB UND TRANSFERIERT ES ZU DER VORRICHTUNG
1208
VORRICHTUNG ERZEUGT ERNEUT EINEN SYMMETRISCHEN SCHLÜSSEL SKEY AUS DEM EINGEBETTETEN RAND-WERT
SKEY = F(RAND)
1210
VORRICHTUNG ENTSCHLÜSSELT LOKALISIERTES SCHLÜSSEL-BLOB MITTELS SKY, UM DPpri UND DPpri-DIGEST ZU ERHALTEN
ENTSCHLÜSSELTES SCHLÜSSEL-BLOB = ENTSCHLÜSSELN (IV2, DPpri, DPpri-DIGEST) MITTELS SKEY
1212
VORRICHTUNG FÜHRT HINSICHTLICH DPpri HASH DURCH, UM DIE INTEGRITÄT DES SCHLÜSSELS MIT PDpri-DIGEST ZU ÜBERPRÜFEN, AKZEPTIERT DPpri FALLS GÜLTIG UND AKTIVIERT DPpri ZUR BENUTZUNG
1214
VORRICHTUNG WÄHLT NEUEN IV UND ERZEUGT NEUES LOKALISIERTES SCHLÜSSEL-BLOB
LOKALISIERTES SCHLÜSSEL-BLOB = VERSCHLÜSSELN (IV3, DPpri; DPpri-DIGEST) MITTELS SKEY
1216
SCHLÜSSELABRUF-UTILITY SPEICHERT NEUES LOKALISIERTES SCHLÜSSEL-BLOB IN CLIENT-COMPUTERSYSTEM-SPEICHER

Figur 12